CWE, CAPEC Integration in Risk Based Threat Modeling

Tony UcedaVelez
CEO, VerSprite

VerSprite
Navigate Beyond Risk

August 31, 2015

Introduction

- Tony UcedaVélez (“Tony UV”)
  - CEO, VerSprite – Global Security Consulting Firm
  - Chapter Leader – OWASP Atlanta (past 7 years)
  - Author, “Risk Centric Threat Modeling – Process for Attack Simulation & Threat Analysis”, Wiley June 2015

What Threat Are You Protecting Against?

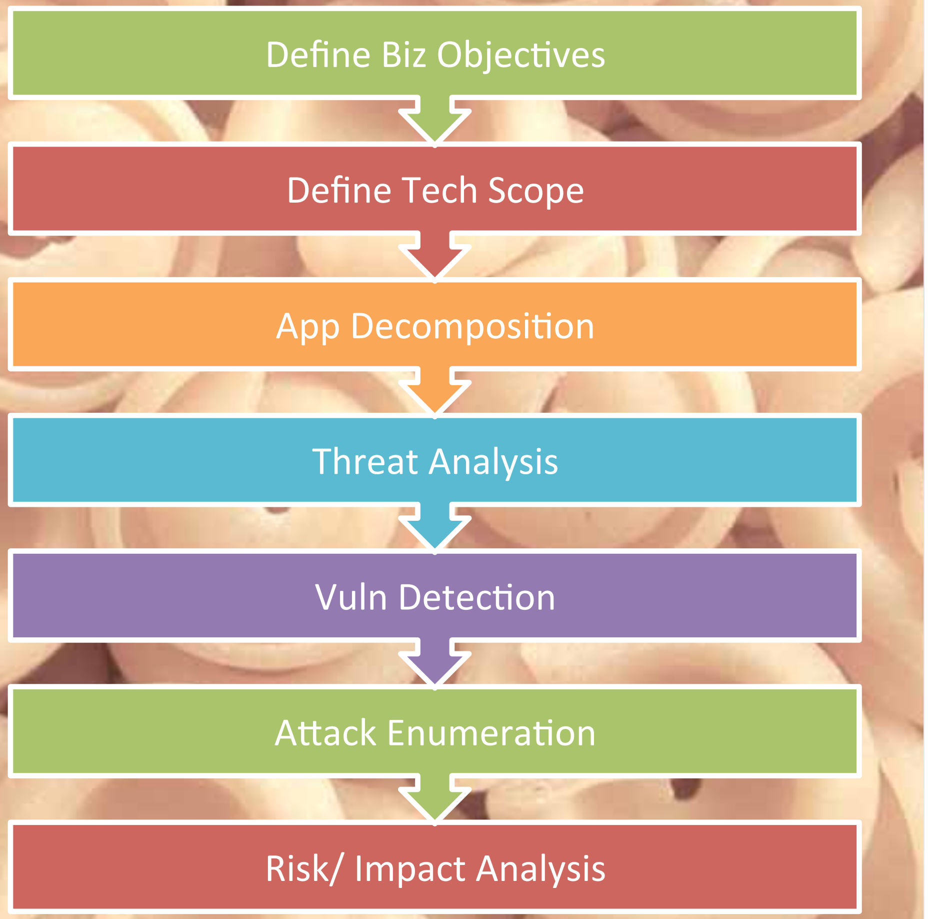
- Do you know who may attack you?
- Do you know why they may attack you?
- Do you know what evidence support your threat claims?
- Use MITRE’s CAPEC & CWE to organize your attack and weakness libraries

PASTA – Risk Centric Threat Modeling

What is PASTA?

- Process for Attack Simulation & Threat Analysis
  - Risk centric threat modeling methodology
  - Collaborative; great for business integration
  - 7 stages building up to impact of threat to application & business.
- Aimed at addressing most viable threats & building security in

A True Methodology (7 Stages)



Define Biz Objectives

Define Tech Scope

App Decomposition

Threat Analysis

Vuln Detection

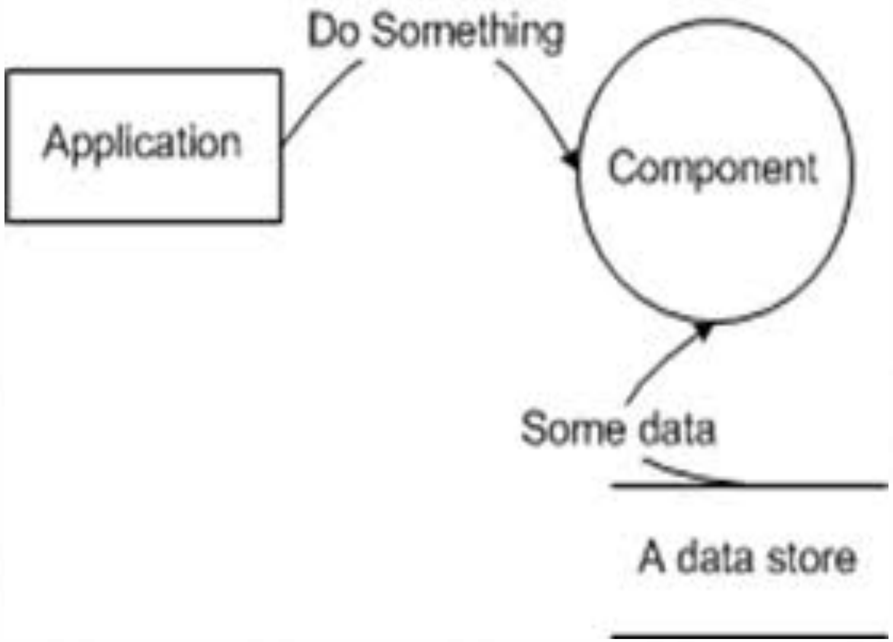
Attack Enumeration

Risk/ Impact Analysis

VerSprite

Threat Modeling

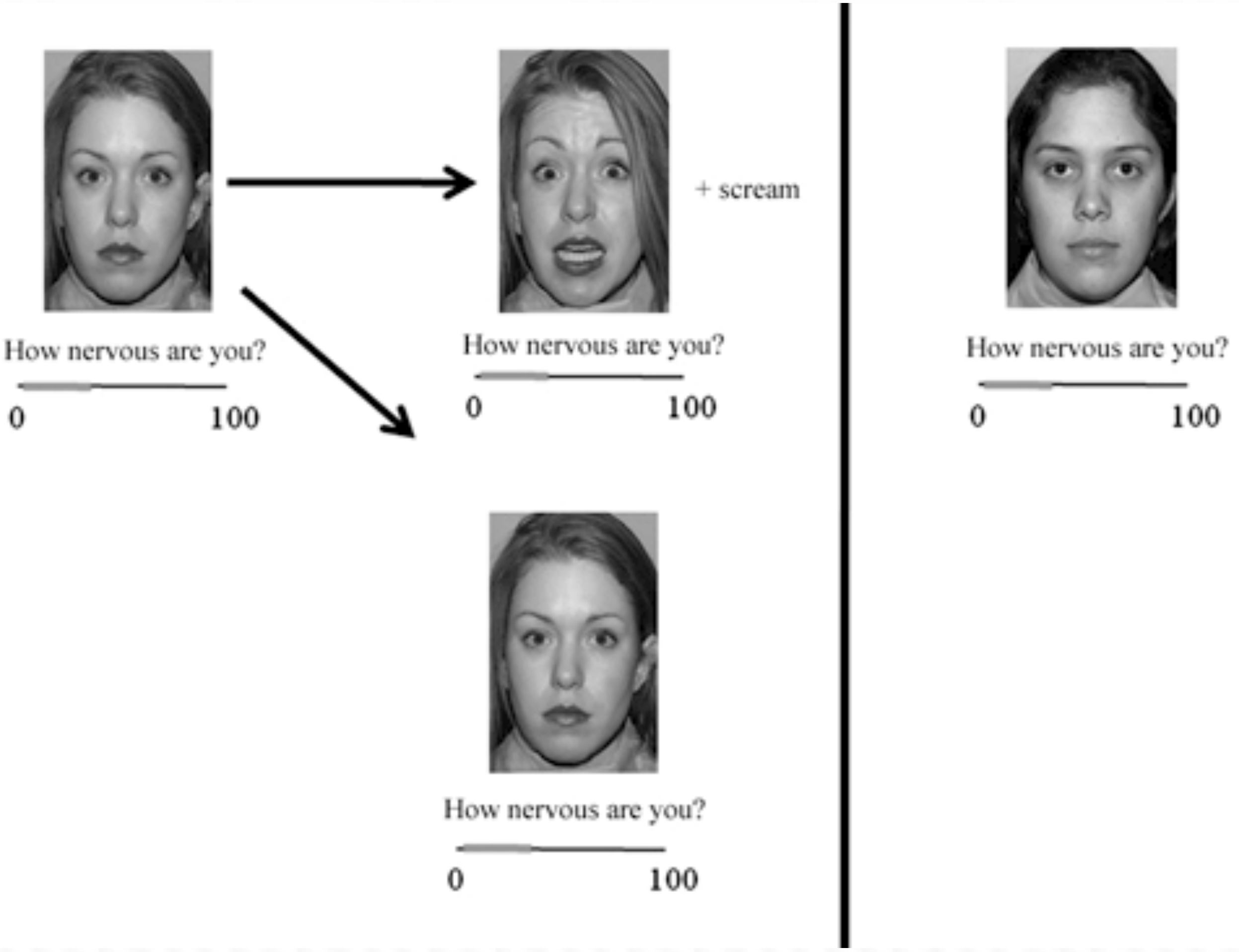
Threat Dissection



Targeted Analysis

- Focused on understanding targeted threats
- Focus on attacks that are supported via viable threat patterns (considering multiple vectors)
- Threat motives may be data (e.g. - PII, IP) focused, disruption based (hacktivism), IP

Threat



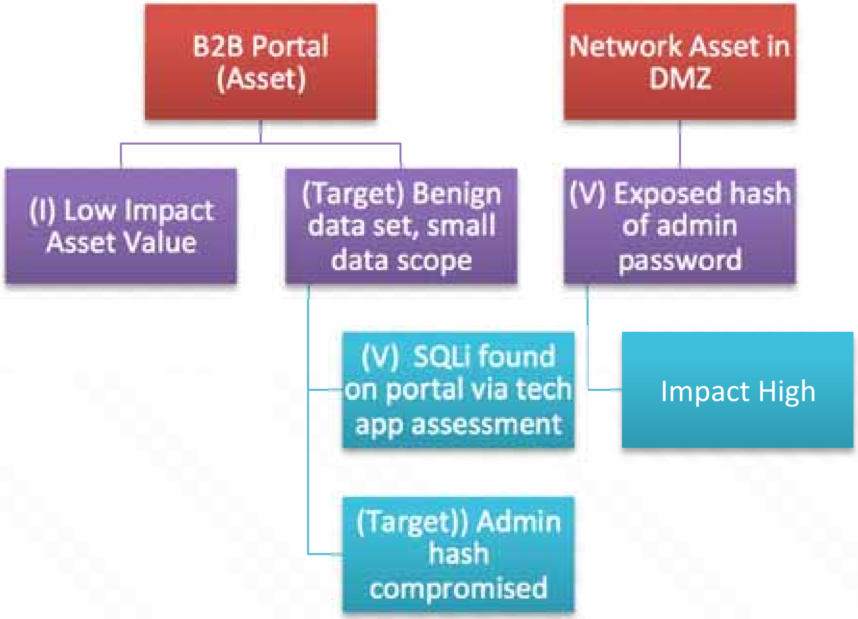
Threat. A threat is an undesired event. A potential occurrence, often best described as causal factors that may manifest into attacks that compromise an asset or objective. Relative to each site, industry, company; more difficult to uniformly define.

Risk Centric Threat Modeling

Risk Management

- Needs to substantiate risks
  - No one believes your risk scores
- Substantiate vulnerable findings w/ threat modeling stages
  - 3 (app decomposition)
  - 4 (threat analysis)
  - 5 (vuln detection) 6 (exploitation)
- Vulnerabilities begin to ‘mean’ something to those who have to remediate them

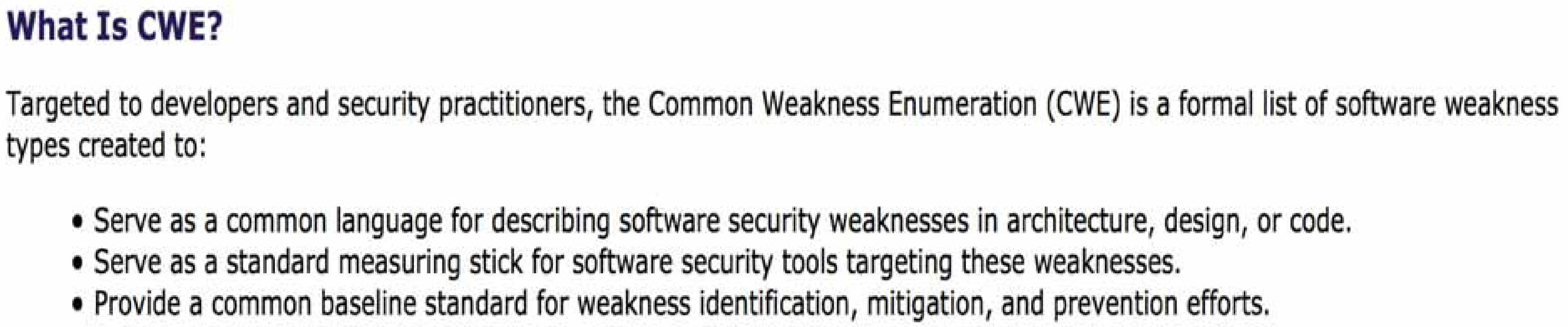
Attack Tree


B2B Portal (Asset)
Network Asset in DMZ
(I) Low Impact Asset Value
(Target) Benign data set, small data scope
(V) Exposed hash of admin password
(V) SQLi found on portal via tech app assessment
Impact High
(Target)) Admin hash compromised

LEVERAGING CAPEC & CWE

VerSprite

What is CWE?

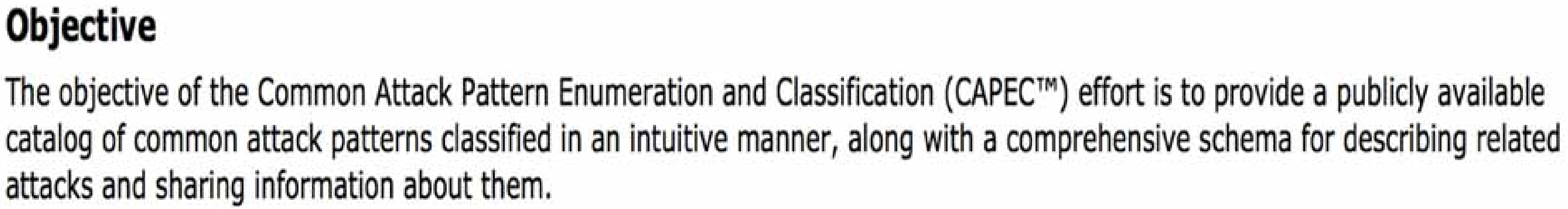


What Is CWE?

Targeted to developers and security practitioners, the Common Weakness Enumeration (CWE) is a formal list of software weakness types created to:

- Serve as a common language for describing software security weaknesses in architecture, design, or code.
- Serve as a standard measuring stick for software security tools targeting these weaknesses.
- Provide a common baseline standard for weakness identification, mitigation, and prevention efforts.

What is CAPEC?



Objective

The objective of the Common Attack Pattern Enumeration and Classification (CAPEC™) effort is to provide a publicly available catalog of common attack patterns classified in an intuitive manner, along with a comprehensive schema for describing related attacks and sharing information about them.

VerSprite

CAPEC Review

Primary Schema Elements

Identifying Information

- Attack Pattern ID
- Attack Pattern Name

Describing Information

- Description
- Related Weaknesses
- Related Vulnerabilities
- Method of Attack
- Examples-Instances
- References

Prescribing Information

- Solutions and Mitigations

Scoping and Delimiting Information

- Typical Severity
- Typical Likelihood of Exploit
- Attack Prerequisites
- Attacker Skill or Knowledge Required
- Resources Required
- Attack Motivation-Consequences
- Context Description

Supporting Schema Elements

Describing Information

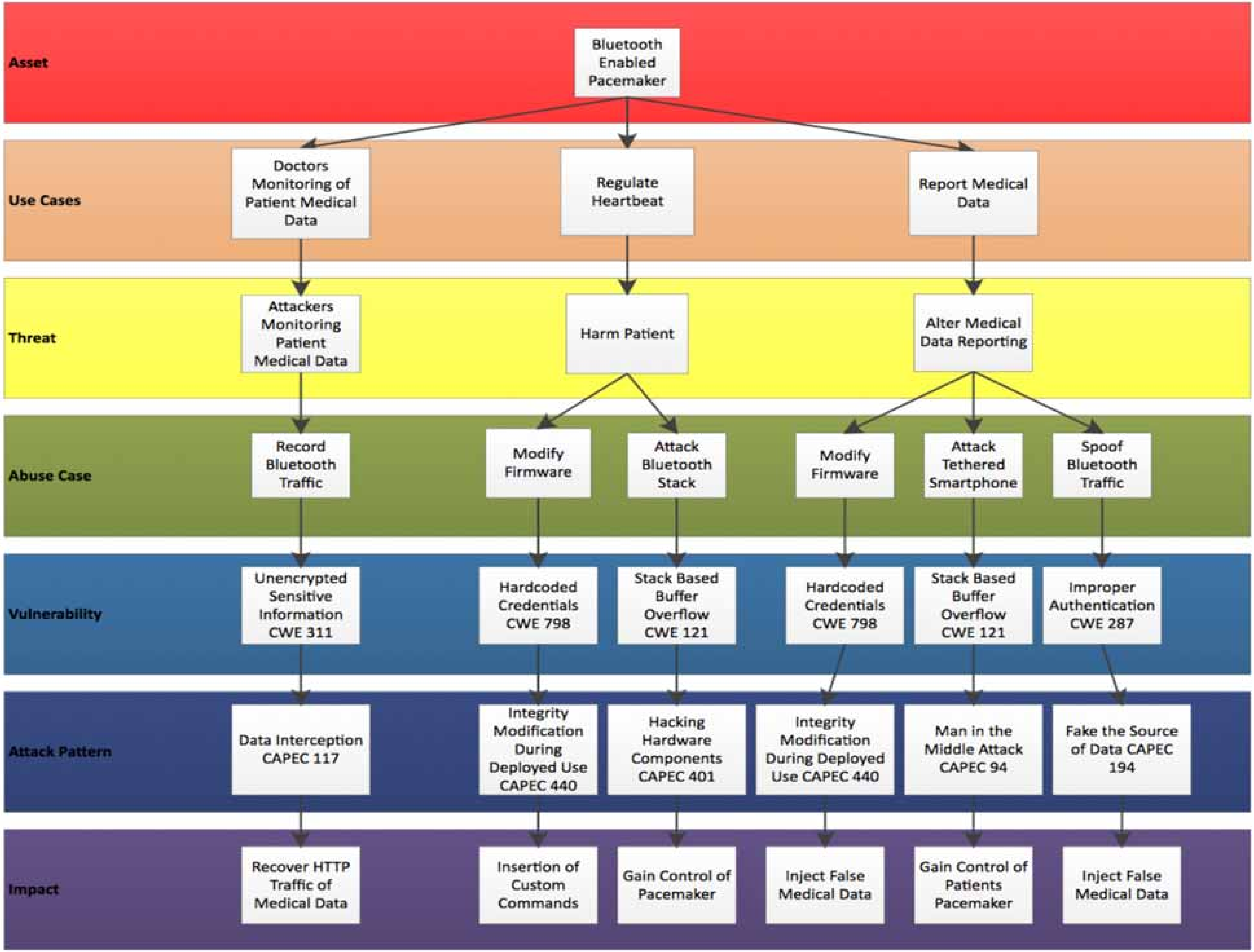
- Injection Vector
- Payload
- Activation Zone
- Payload Activation Impact

Diagnosing Information

- Probing Techniques
- Indicators-Warnings of Attack
- Obfuscation Techniques

Enhancing Information

- Related Attack Patterns
- Relevant Security Requirements
- Relevant Design Patterns
- Relevant Security Patterns



Asset

Bluetooth Enabled Pacemaker

Use Cases

Doctors Monitoring of Patient Medical Data

Regulate Heartbeat

Report Medical Data

Threat

Attackers Monitoring Patient Medical Data

Harm Patient

Alter Medical Data Reporting

Abuse Case

Record Bluetooth Traffic

Modify Firmware

Attack Bluetooth Stack

Modify Firmware

Attack Tethered Smartphone

Spoof Bluetooth Traffic

Vulnerability

Unencrypted Sensitive Information CWE 311

Hardcoded Credentials CWE 798

Stack Based Buffer Overflow CWE 121

Hardcoded Credentials CWE 798

Stack Based Buffer Overflow CWE 121

Improper Authentication CWE 287

Attack Pattern

Data Interception CAPEC 117

Integrity Modification During Deployed Use CAPEC 440

Hacking Hardware Components CAPEC 401

Integrity Modification During Deployed Use CAPEC 440

Man in the Middle Attack CAPEC 94

Fake the Source of Data CAPEC 194

Impact

Recover HTTP Traffic of Medical Data

Insertion of Custom Commands

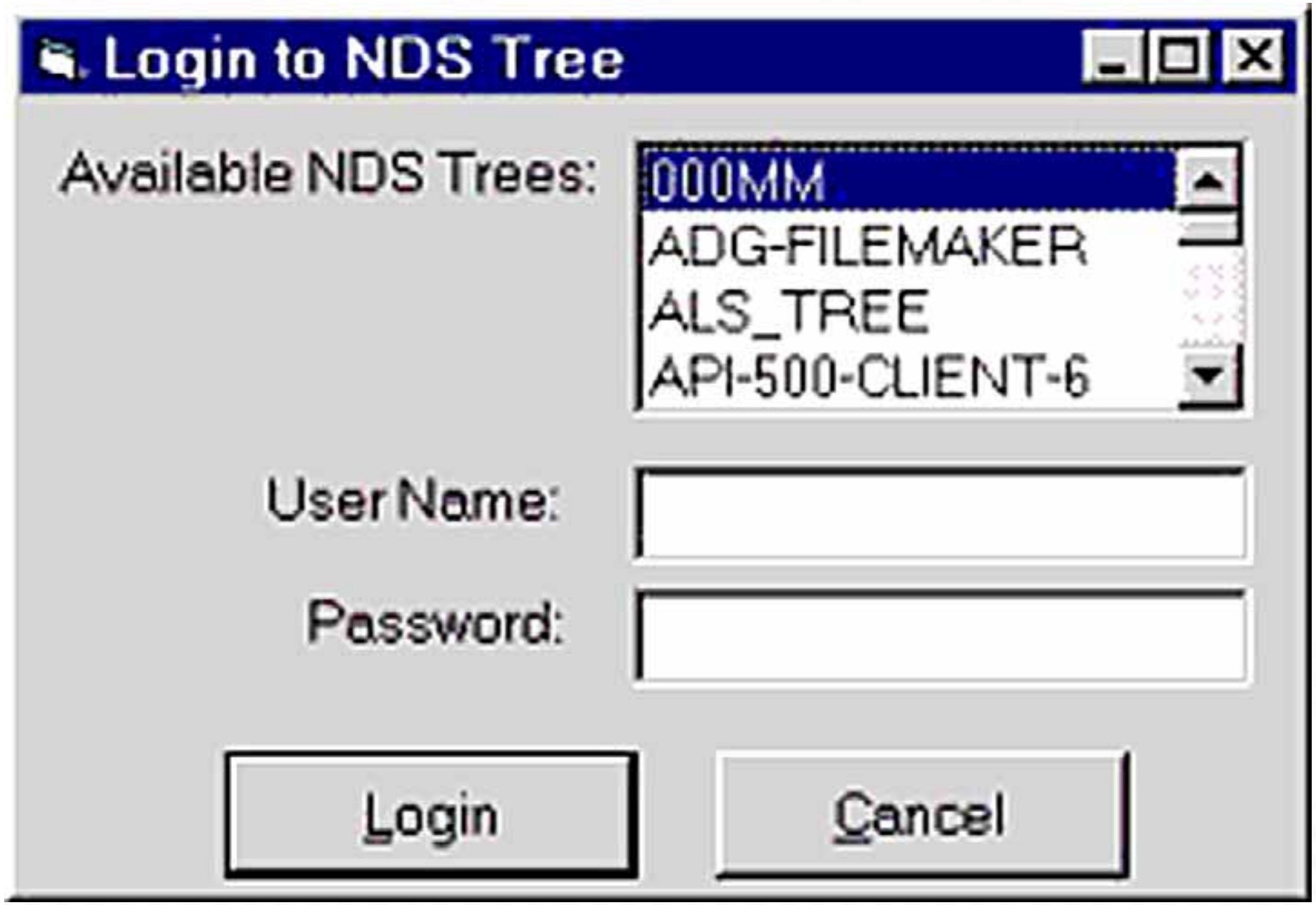
Gain Control of Pacemaker

Inject False Medical Data

Gain Control of Patients Pacemaker

Inject False Medical Data

Use Case



Login to NDS Tree

Available NDS Trees:

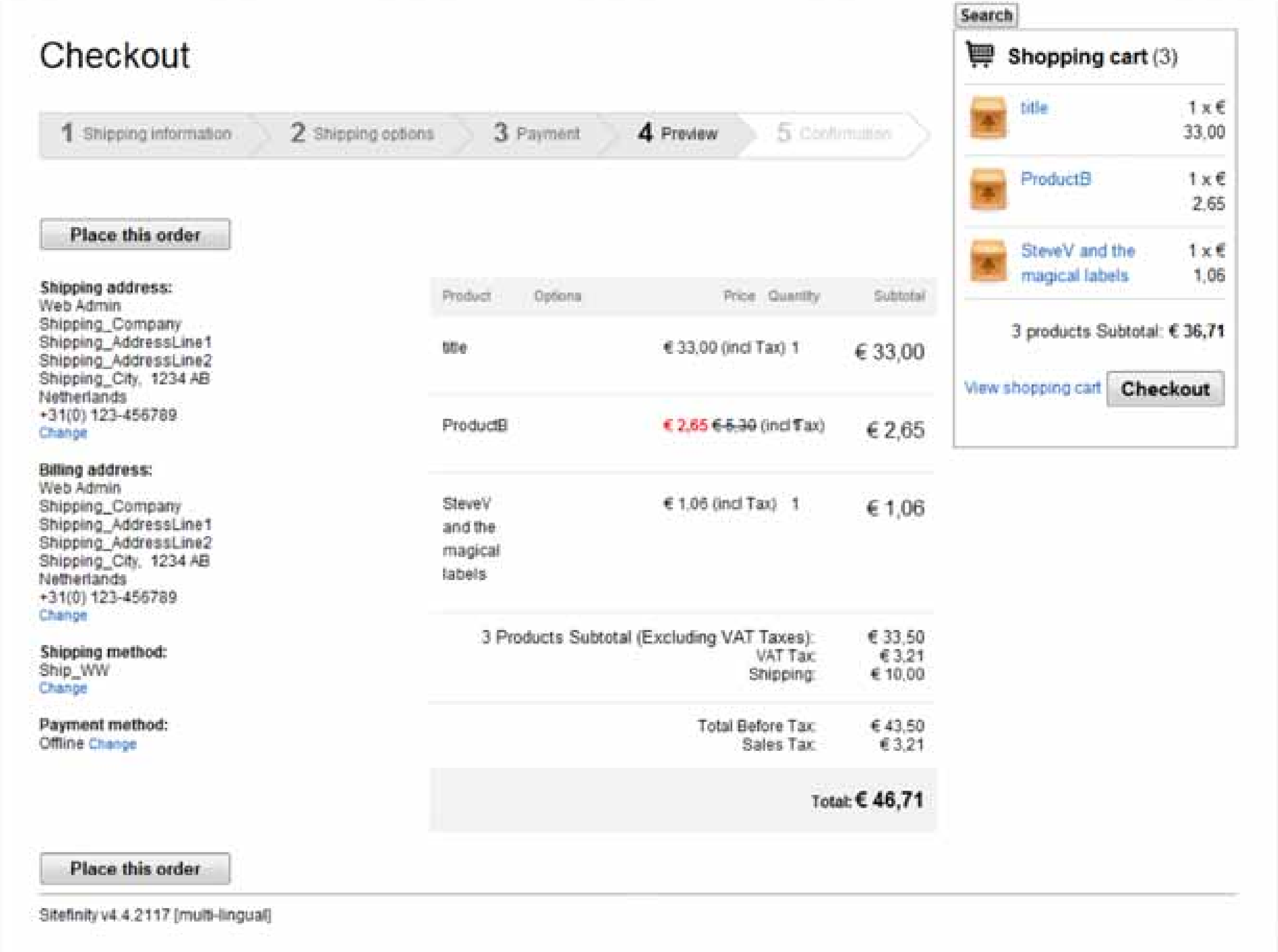
- 000MM
- ADG-FILEMAKER
- ALS_TREE
- API-500-CLIENT-6

User Name:

Password:

Use Case. Functional, as designed function of an application.

Abuse Case



Checkout

1 Shipping information | 2 Shipping options | 3 Payment | 4 Preview | 5 Confirmation

Place this order

Shipping address:
Web Admin
Shipping_Company
Shipping_AddressLine1
Shipping_AddressLine2
Shipping_City, 1234 AB
Netherlands
+31(0) 123-456789
Change

Billing address:
Web Admin
Shipping_Company
Shipping_AddressLine1
Shipping_AddressLine2
Shipping_City, 1234 AB
Netherlands
+31(0) 123-456789
Change

Shipping method:
Ship_WW
Change

Payment method:
Offline Change

Product	Options	Price	Quantity	Subtotal
title		€ 33,00 (incl Tax)	1	€ 33,00
ProductB		€ 2,65 ~~€ 5,30~~ (incl Tax)		€ 2,65
SteveV and the magical labels		€ 1,06 (incl Tax)	1	€ 1,06

3 Products Subtotal (Excluding VAT Taxes):	€ 33,50
VAT Tax:	€ 3,21
Shipping:	€ 10,00
Total Before Tax:	€ 43,50
Sales Tax:	€ 3,21
Total: € 46,71	

Place this order

Sitefinity v4.4.2117 [multi-lingual]

Search

Shopping cart (3)

title	1 x € 33,00
ProductB	1 x € 2,65
SteveV and the magical labels	1 x € 1,06

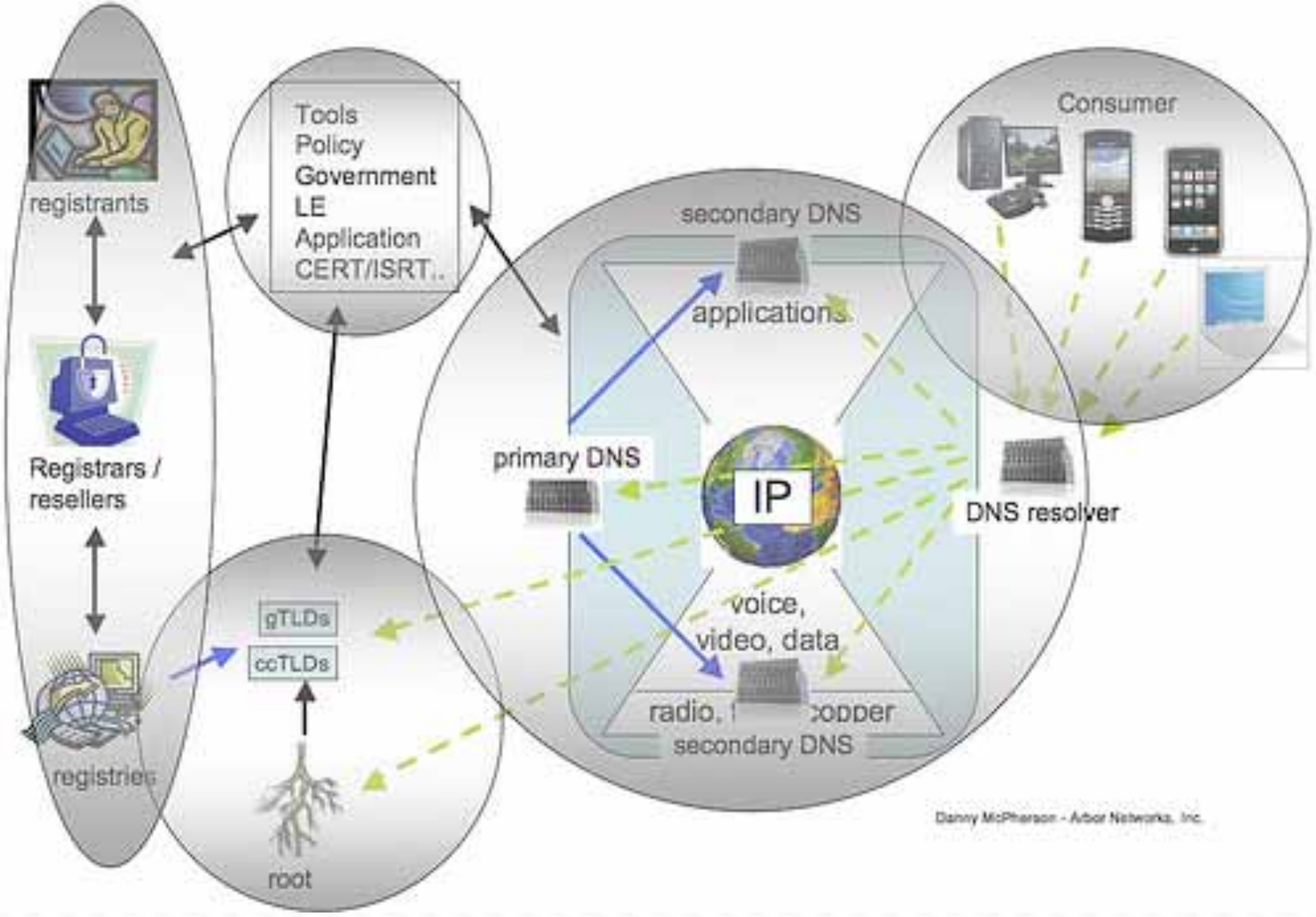
3 products Subtotal: **€ 36,71**

View shopping cart Checkout

Abuse Case. Deliberate abuse of functional use cases in order to yield unintended results

VerSprite

Attack Surface

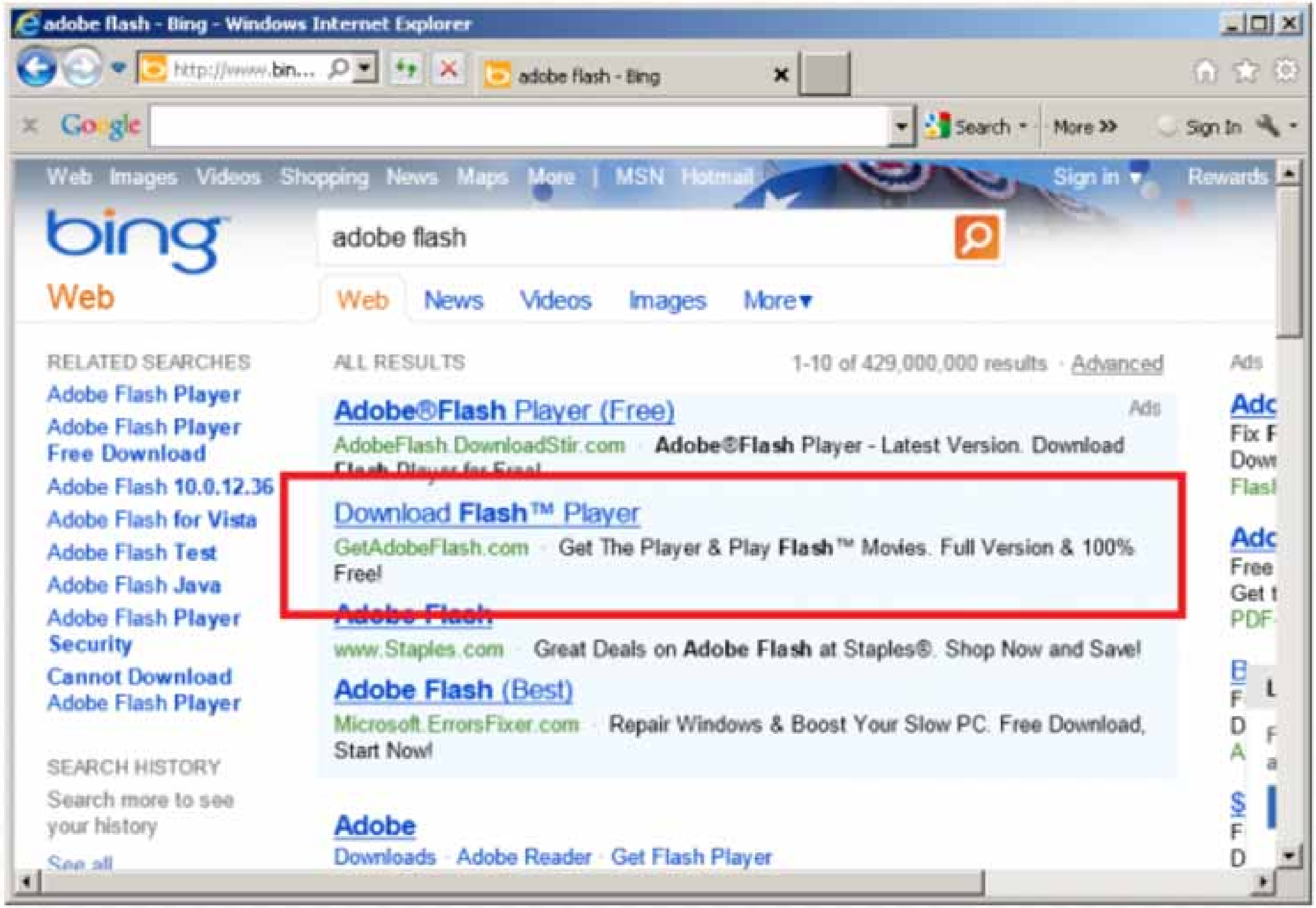


Danny McPherson - Arbor Networks, Inc.

Attack Surface. Logical area (browser stack, infrastructure components, etc) or physical area (hotel kiosk).

Where do you define this in risk assessments or compliance audits?

Attack Vector


adobe flash - Bing - Windows Internet Explorer
http://www.bin...
adobe flash - Bing
Google
Search
More »
Sign In
Web Images Videos Shopping News Maps More | MSN Hotmail
Sign in
Rewards
bing
adobe flash
Web
Web News Videos Images More▾

RELATED SEARCHES

Adobe Flash Player

Adobe Flash Player Free Download

Adobe Flash 10.0.12.36

Adobe Flash for Vista

Adobe Flash Test

Adobe Flash Java

Adobe Flash Player Security

Cannot Download Adobe Flash Player

SEARCH HISTORY

Search more to see your history

See all

ALL RESULTS 1-10 of 429,000,000 results · Advanced

Ads

Adobe®Flash Player (Free)

AdobeFlash.DownloadStir.com · Adobe®Flash Player - Latest Version. Download Flash Player for Free!

Download Flash™ Player

GetAdobeFlash.com · Get The Player & Play Flash™ Movies. Full Version & 100% Free!

Adobe Flash

www.Staples.com · Great Deals on Adobe Flash at Staples®. Shop Now and Save!

Adobe Flash (Best)

Microsoft.ErrorsFixer.com · Repair Windows & Boost Your Slow PC. Free Download, Start Now!

Adobe

Downloads · Adobe Reader · Get Flash Player

Ads

Adc

Fix F

Dow

Flas

Adc

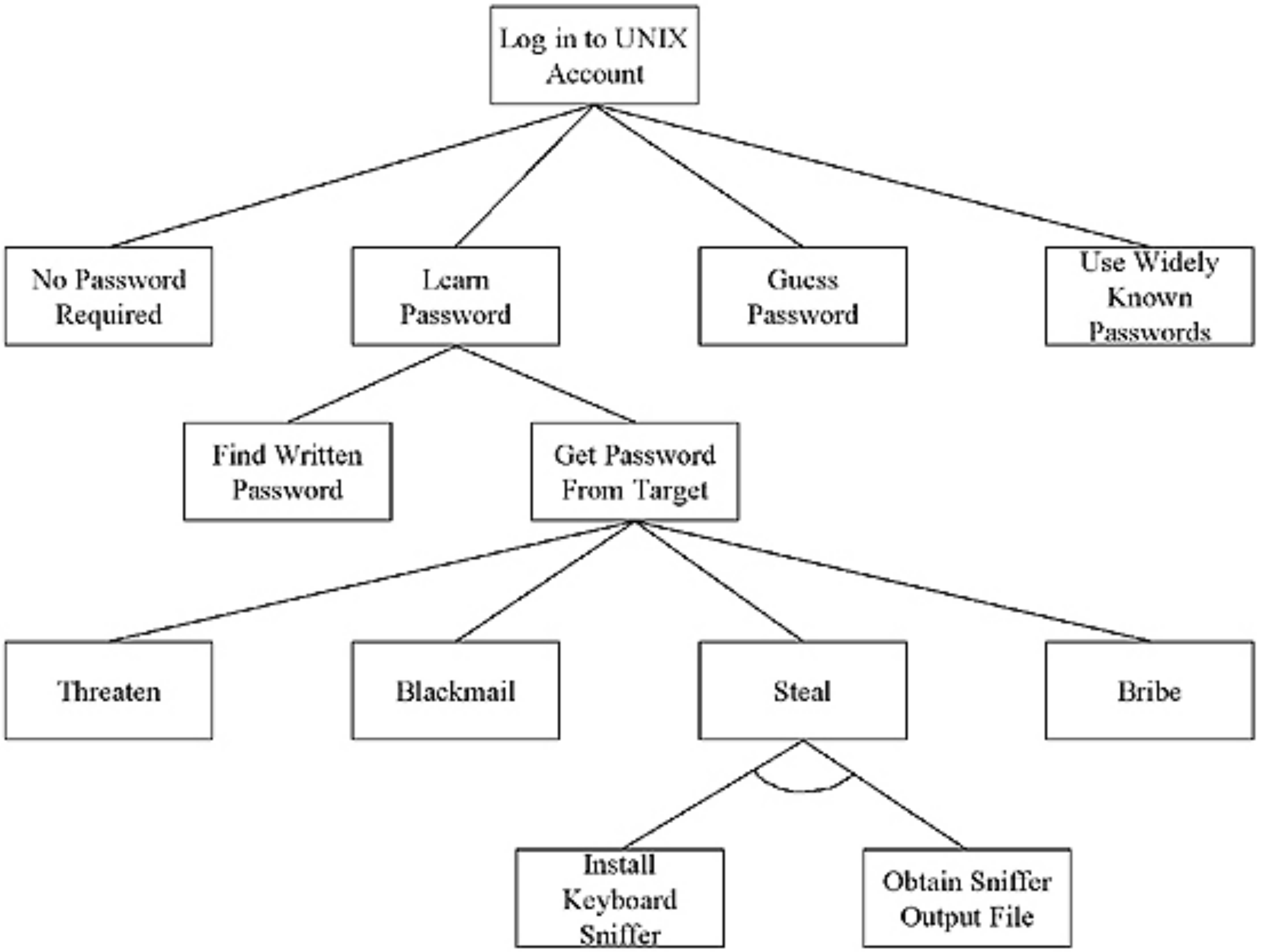
Free

Get t

PDF

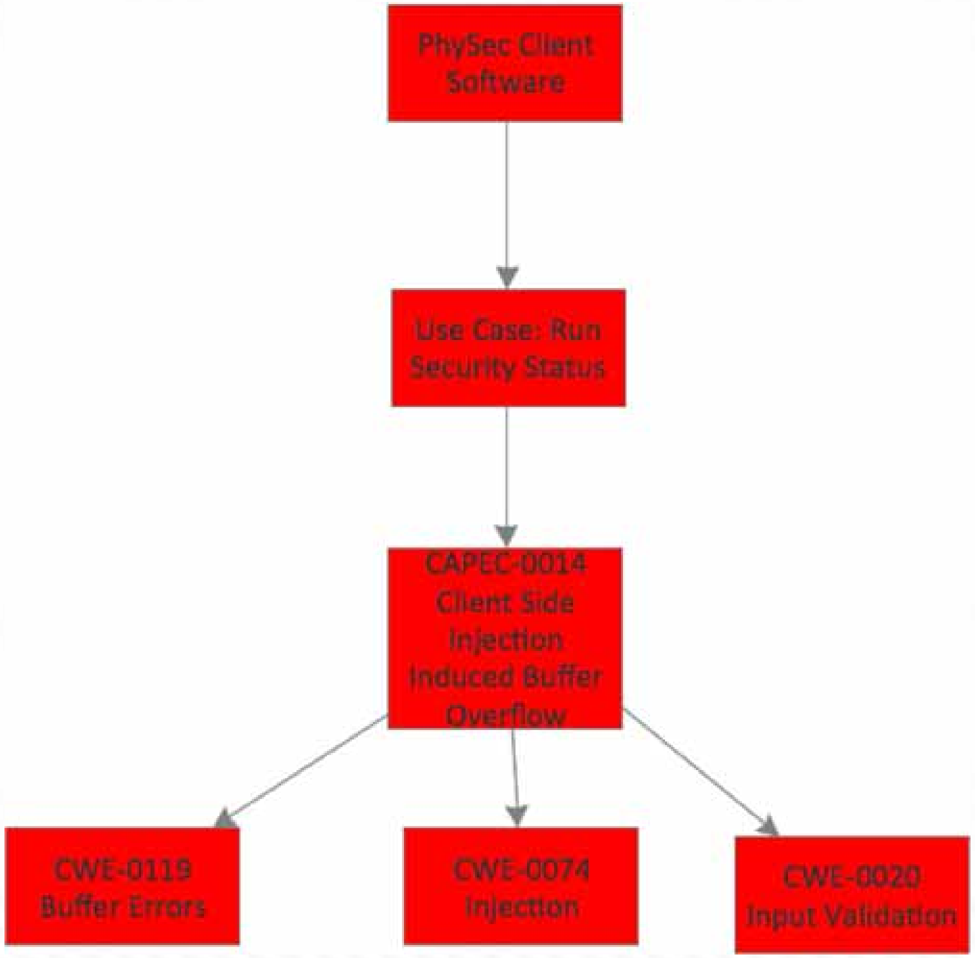
Attack Vector. Point & channel for which attacks travel over (card reader, form fields, network proxy, client browser, etc)

Attack Trees



Attack Tree. Helpful diagram of relationship amongst asset-actor-use case-abuse case-vuln-exploit-countermeasure

CAPEC + CWE Use in Attack Trees



PhySec Client Software

Use Case: Run Security Status

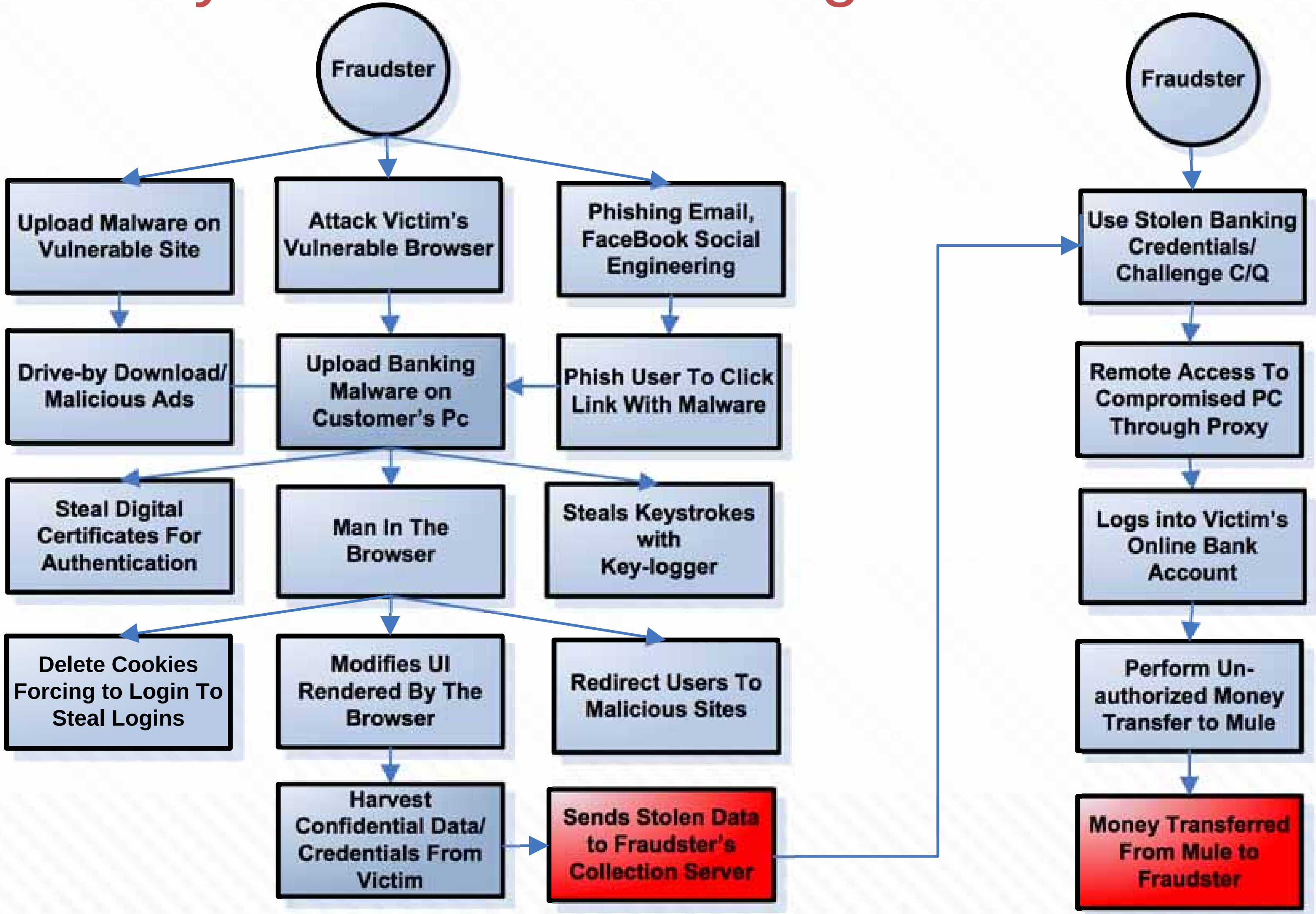
CAPEC-0014 Client Side Injection Induced Buffer Overflow

CWE-0119 Buffer Errors

CWE-0074 Injection

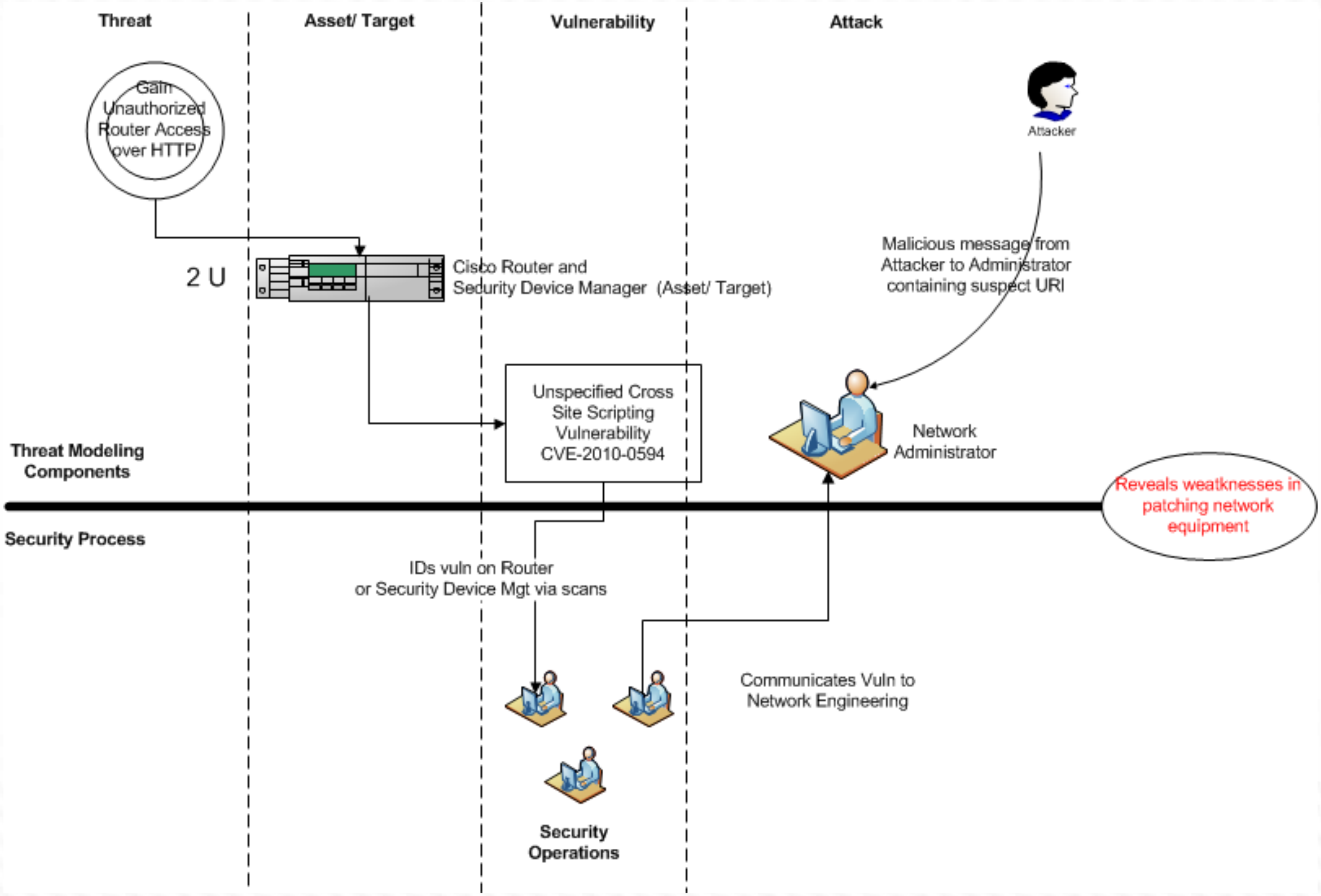
CWE-0020 Input Validation

Analysis Of Attacks Using Attack Trees


Fraudster
Upload Malware on Vulnerable Site
Attack Victim's Vulnerable Browser
Phishing Email, FaceBook Social Engineering
Drive-by Download/ Malicious Ads
Upload Banking Malware on Customer's Pc
Phish User To Click Link With Malware
Steal Digital Certificates For Authentication
Man In The Browser
Steals Keystrokes with Key-logger
Delete Cookies Forcing to Login To Steal Logins
Modifies UI Rendered By The Browser
Redirect Users To Malicious Sites
Harvest Confidential Data/ Credentials From Victim
Sends Stolen Data to Fraudster's Collection Server
Fraudster
Use Stolen Banking Credentials/ Challenge C/Q
Remote Access To Compromised PC Through Proxy
Logs into Victim's Online Bank Account
Perform Un-authorized Money Transfer to Mule
Money Transferred From Mule to Fraudster

VerSprite

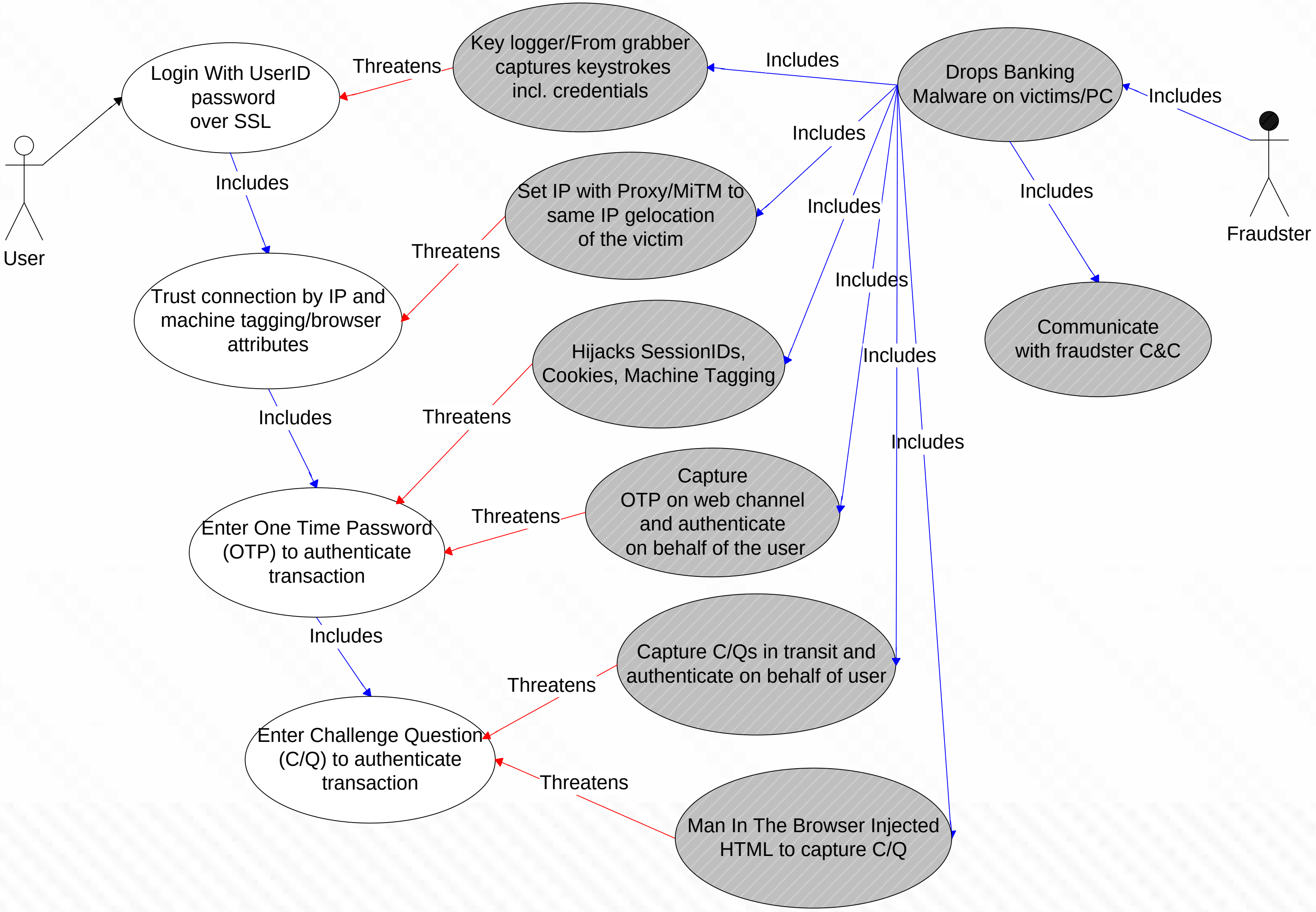
Attack Model



Threat
Asset/ Target
Vulnerability
Attack
Gain Unauthorized Router Access over HTTP
Attacker
2 U
Cisco Router and Security Device Manager (Asset/ Target)
Malicious message from Attacker to Administrator containing suspect URI
Unspecified Cross Site Scripting Vulnerability CVE-2010-0594
Network Administrator
Threat Modeling Components
Reveals weatknesses in patching network equipment
Security Process
IDs vuln on Router or Security Device Mgt via scans
Communicates Vuln to Network Engineering
Security Operations

VerSprite

Layered Attacks to Thwart Countermeasures

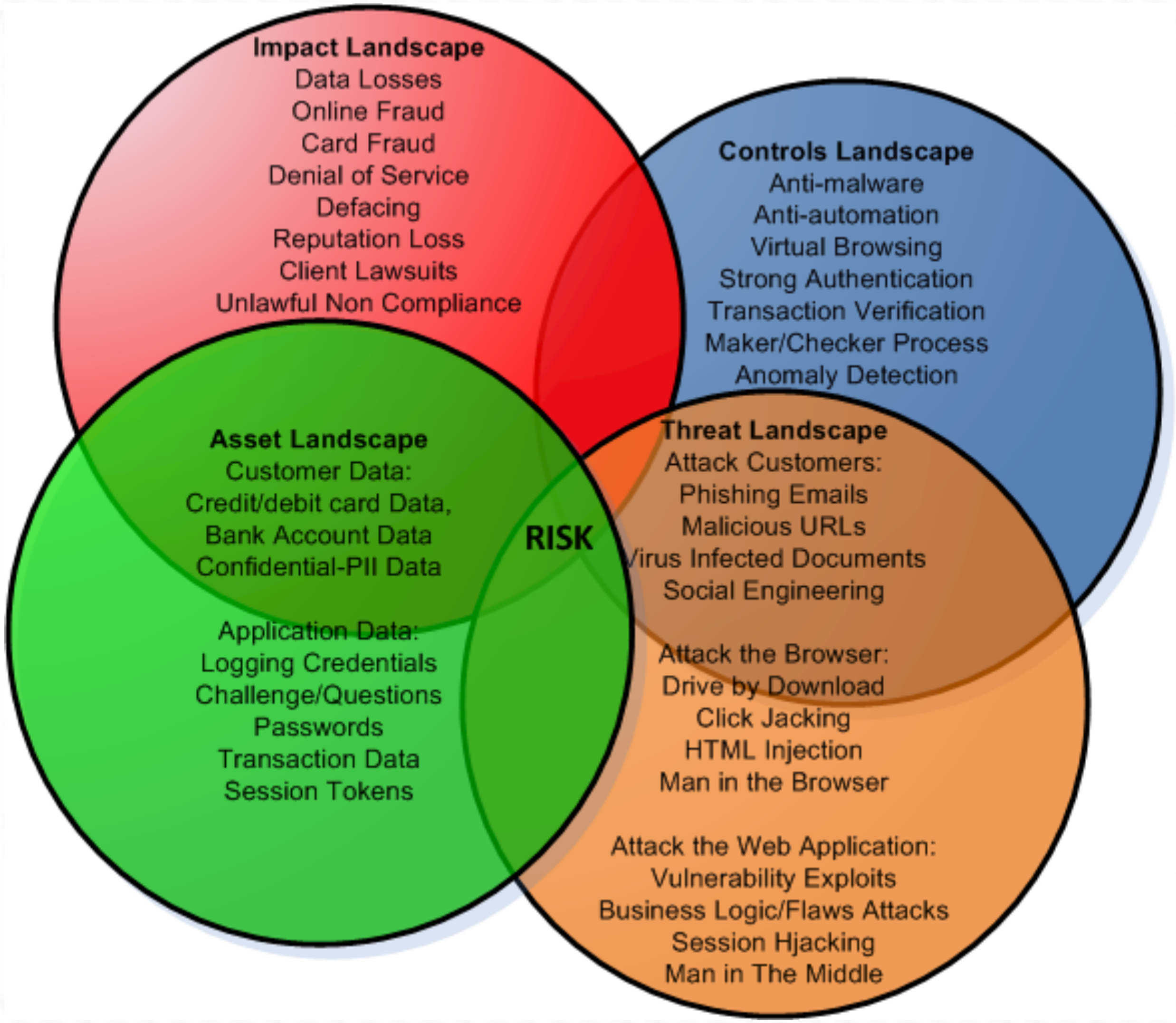

User
Login With UserID password over SSL
Includes
Trust connection by IP and machine tagging/browser attributes
Includes
Enter One Time Password (OTP) to authenticate transaction
Includes
Enter Challenge Question (C/Q) to authenticate transaction
Threatens
Key logger/From grabber captures keystrokes incl. credentials
Threatens
Set IP with Proxy/MiTM to same IP gelocation of the victim
Threatens
Hijacks SessionIDs, Cookies, Machine Tagging
Threatens
Capture OTP on web channel and authenticate on behalf of the user
Threatens
Capture C/Qs in transit and authenticate on behalf of user
Threatens
Man In The Browser Injected HTML to capture C/Q
Includes
Includes
Includes
Includes
Includes
Includes
Drops Banking Malware on victims/PC
Includes
Includes
Communicate with fraudster C&C
Fraudster

OWASP Tie-In

- **OWASP WASC Web Hacking Incidents Database Project**
  - project dedicated to maintaining a list of web applications related security incidents.
  - https://www.owasp.org/index.php/OWASP_WASC_Web_Hacking_Incidents_Database_Project
- **OWASP Security Knowledge Framework**
  - a tool that is used as a guide for building and verifying secure software. It can also be used to train developers about application security.
  - https://www.owasp.org/index.php/OWASP_Security_Knowledge_Framework#tab=Main
  - Incorporates Applications Security Verification Standard
    - https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project

VerSprite

Security Convergence via PASTA



Impact Landscape
Data Losses
Online Fraud
Card Fraud
Denial of Service
Defacing
Reputation Loss
Client Lawsuits
Unlawful Non Compliance

Controls Landscape
Anti-malware
Anti-automation
Virtual Browsing
Strong Authentication
Transaction Verification
Maker/Checker Process
Anomaly Detection

Asset Landscape
Customer Data:
Credit/debit card Data,
Bank Account Data
Confidential-PII Data

Application Data:
Logging Credentials
Challenge/Questions
Passwords
Transaction Data
Session Tokens

RISK

Threat Landscape
Attack Customers:
Phishing Emails
Malicious URLs
Virus Infected Documents
Social Engineering

Attack the Browser:
Drive by Download
Click Jacking
HTML Injection
Man in the Browser

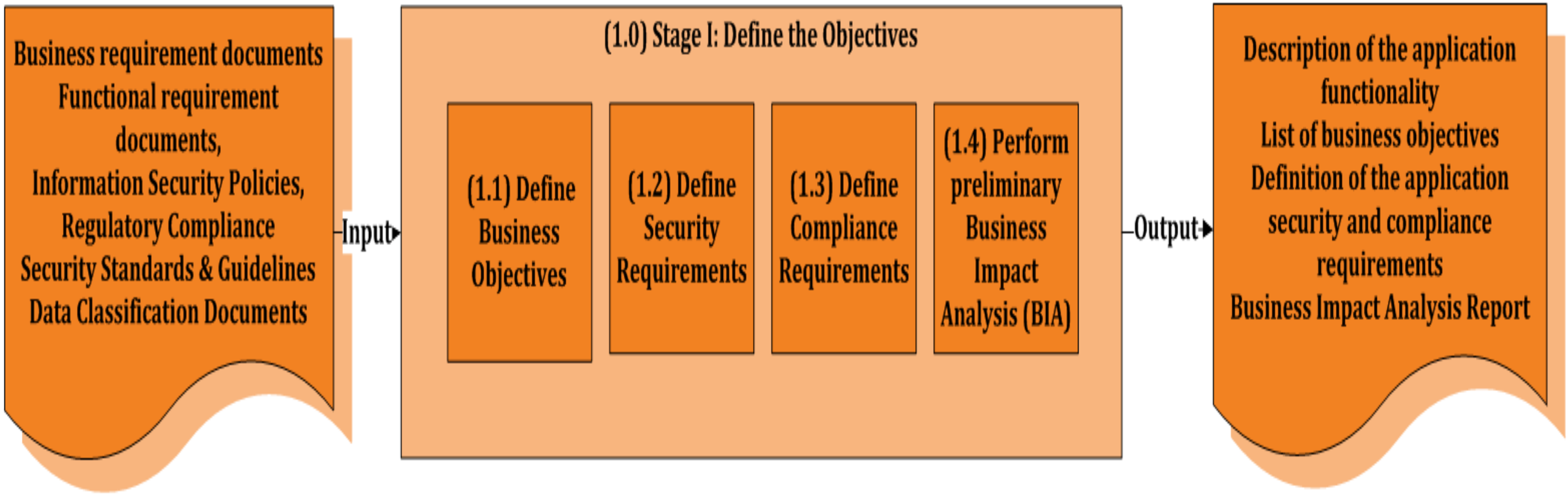
Attack the Web Application:
Vulnerability Exploits
Business Logic/Flaws Attacks
Session Hjacking
Man in The Middle

Source*: Risk Centric Threat Modeling, UcedaVelez, Morana 2015, Chapter V, Threat Modeling & Risk Management ,Wiley*

PASTA METHODOLOGY

VerSprite

Stage 1 – Understand Biz Objectives behind Security, Compliance



Business requirement documents
Functional requirement documents,
Information Security Policies,
Regulatory Compliance
Security Standards & Guidelines
Data Classification Documents

Input

(1.0) Stage I: Define the Objectives

(1.1) Define Business Objectives

(1.2) Define Security Requirements

(1.3) Define Compliance Requirements

(1.4) Perform preliminary Business Impact Analysis (BIA)

Output

Description of the application functionality
List of business objectives
Definition of the application security and compliance requirements
Business Impact Analysis Report

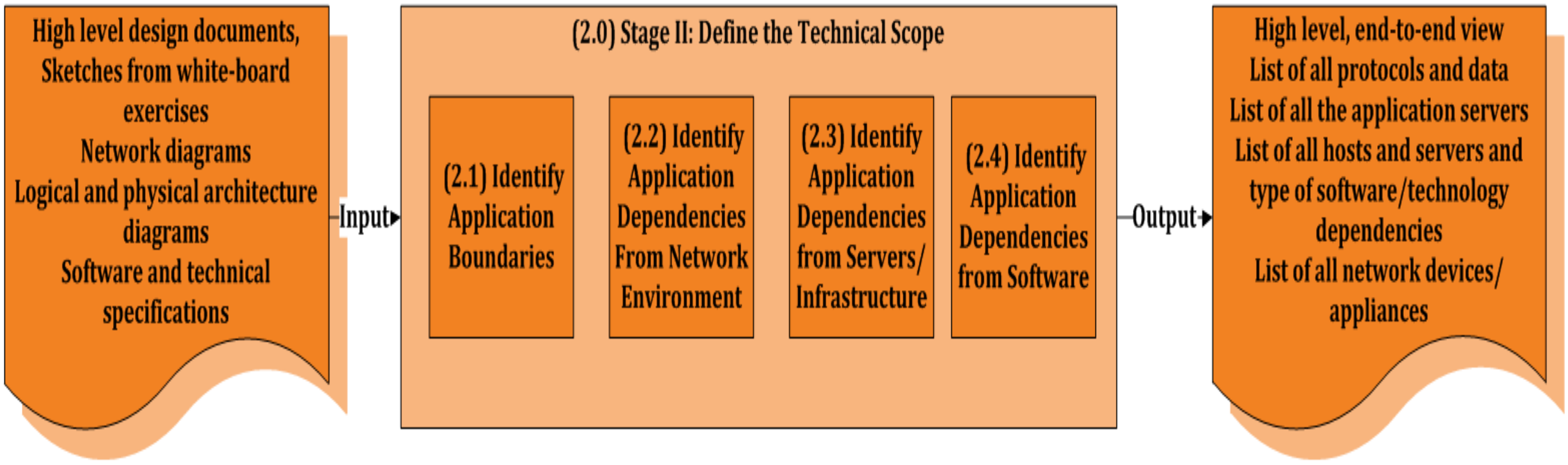
Baking in GRC

- Serve as inherent countermeasures in the form of people, process, technology
  - Policies (for people)
  - Standards (for technology)
- Prior risk assessments help build app risk profile
  - Historical RAs provide prior risk profile of app
- Regulatory landscape taken into consideration, but not the driver
  - Key here is to not retrofit compliance; more costly
- Web Related Example:
  - Tech: Using Nessus OWASP template to audit for PHP & ColdFusion hardening guidelines
  - OWASP Input Validation Cheat Sheets
  - CIS Web Technology Benchmarks

Threat Modeling Stage 1 Artifact

Application Profile: Online Banking Application	
General Description	The online banking application allows customers to perform banking activities such as financial transactions over the internet. The type of transactions supported by the application includes bill payments, wires, funds transfers between customer's own accounts and other bank institutions, account balance-inquires, transaction inquires, bank statements, new bank accounts loan and credit card applications. New online customers can register an online account using existing debit card, PIN and account information. Customers authenticate to the application using username and password and different types of Multi Factor Authentication (MFA) and Risk Based Authentication (RBA)
Application Type	Internet Facing
Data Classification	Public, Non Confidential, Sensitive and Confidential PII
Inherent Risk	HIGH (Infrastructure , Limited Trust Boundary, Platform Risks, Accessability)
High Risk Transactions	YES
User roles	Visitor, customer, administrator, customer support representative
Number of users	3 million registered customers

Stage 2 Walkthru – Define Tech Scope



High level design documents,
Sketches from white-board exercises
Network diagrams
Logical and physical architecture diagrams
Software and technical specifications

Input

(2.0) Stage II: Define the Technical Scope

(2.1) Identify Application Boundaries

(2.2) Identify Application Dependencies From Network Environment

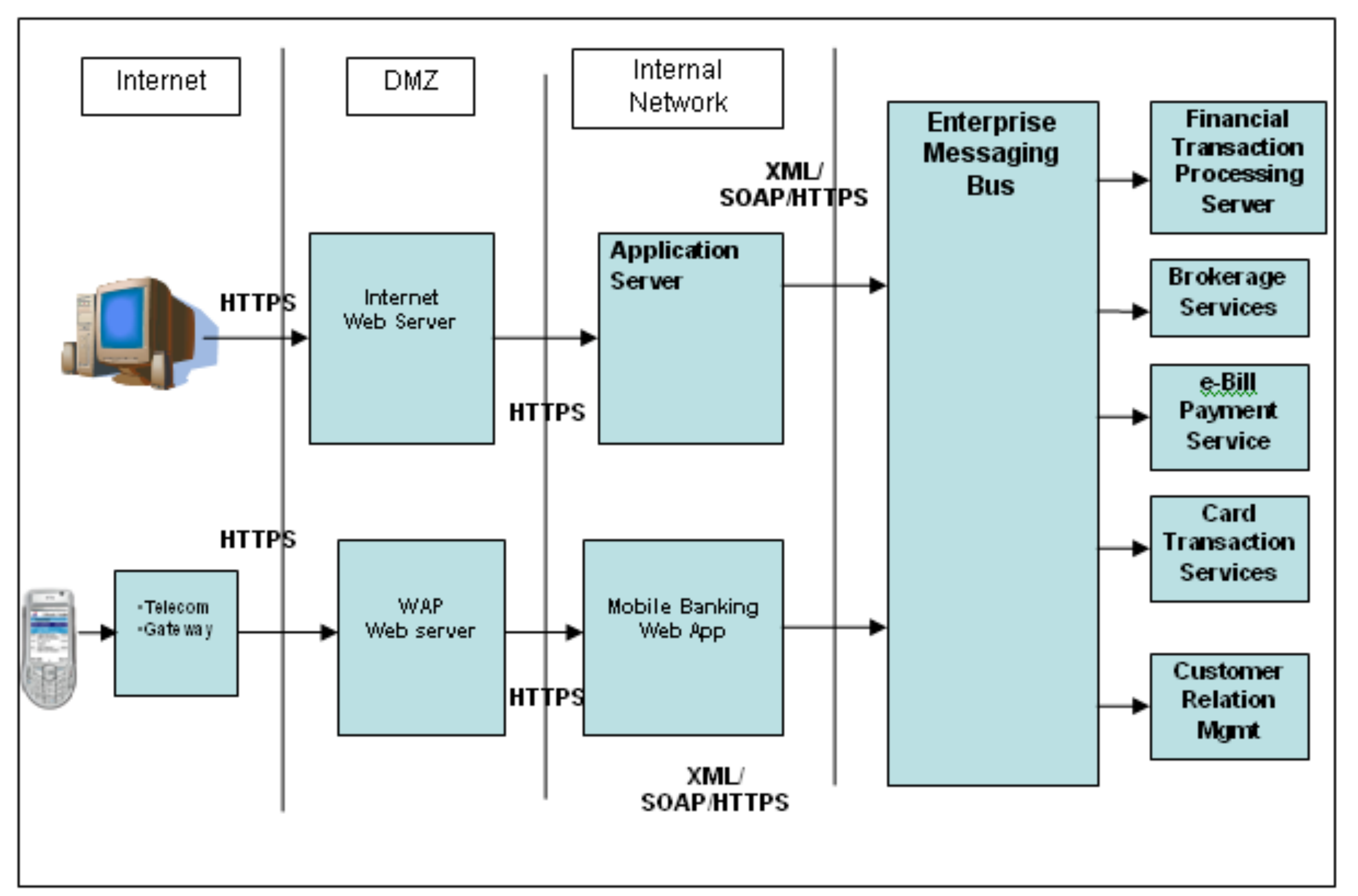
(2.3) Identify Application Dependencies from Servers/ Infrastructure

(2.4) Identify Application Dependencies from Software

Output

High level, end-to-end view
List of all protocols and data
List of all the application servers
List of all hosts and servers and type of software/technology dependencies
List of all network devices/ appliances

The Application Architecture Scope



Technical Scope Definition

Define the scope from design artifacts:

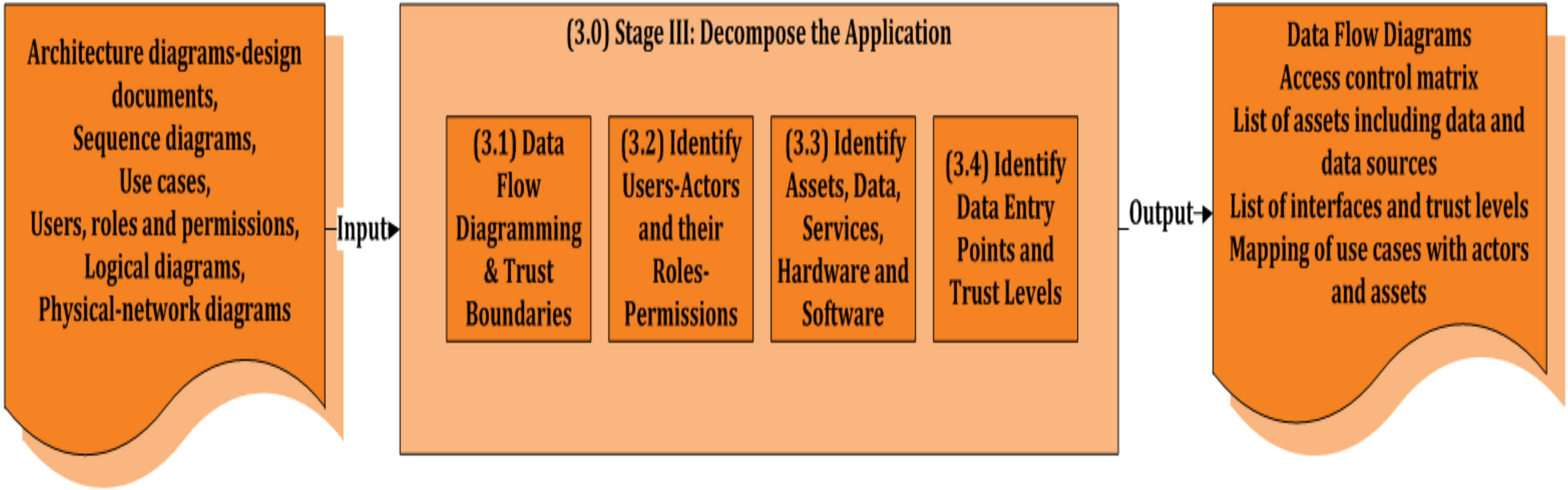
- **Application components** with respect to the application tiers (presentation, application, data)
- **Network topology**
- **Protocol/services** being used/exposed from/to the user to/from the back end (e.g. data flow diagrams)
- **Use case scenarios** (e.g. sequence diagrams)

Model the application in support of security architecture risk analysis

- **The application assets** (e.g. data/services at each tier)
- **The security controls of the application** (e.g. authentication, authorization, encryption, session management, input validation, auditing and logging)
- **Data interactions** between the user of the application and between servers for the main use case scenarios (e.g. login, registration, query etc)

VerSprite
Navigate Beyond Risk

Stage 3– App Decomposition



Architecture diagrams-design documents,
Sequence diagrams,
Use cases,
Users, roles and permissions,
Logical diagrams,
Physical-network diagrams

Input

(3.0) Stage III: Decompose the Application

(3.1) Data Flow Diagramming & Trust Boundaries

(3.2) Identify Users-Actors and their Roles-Permissions

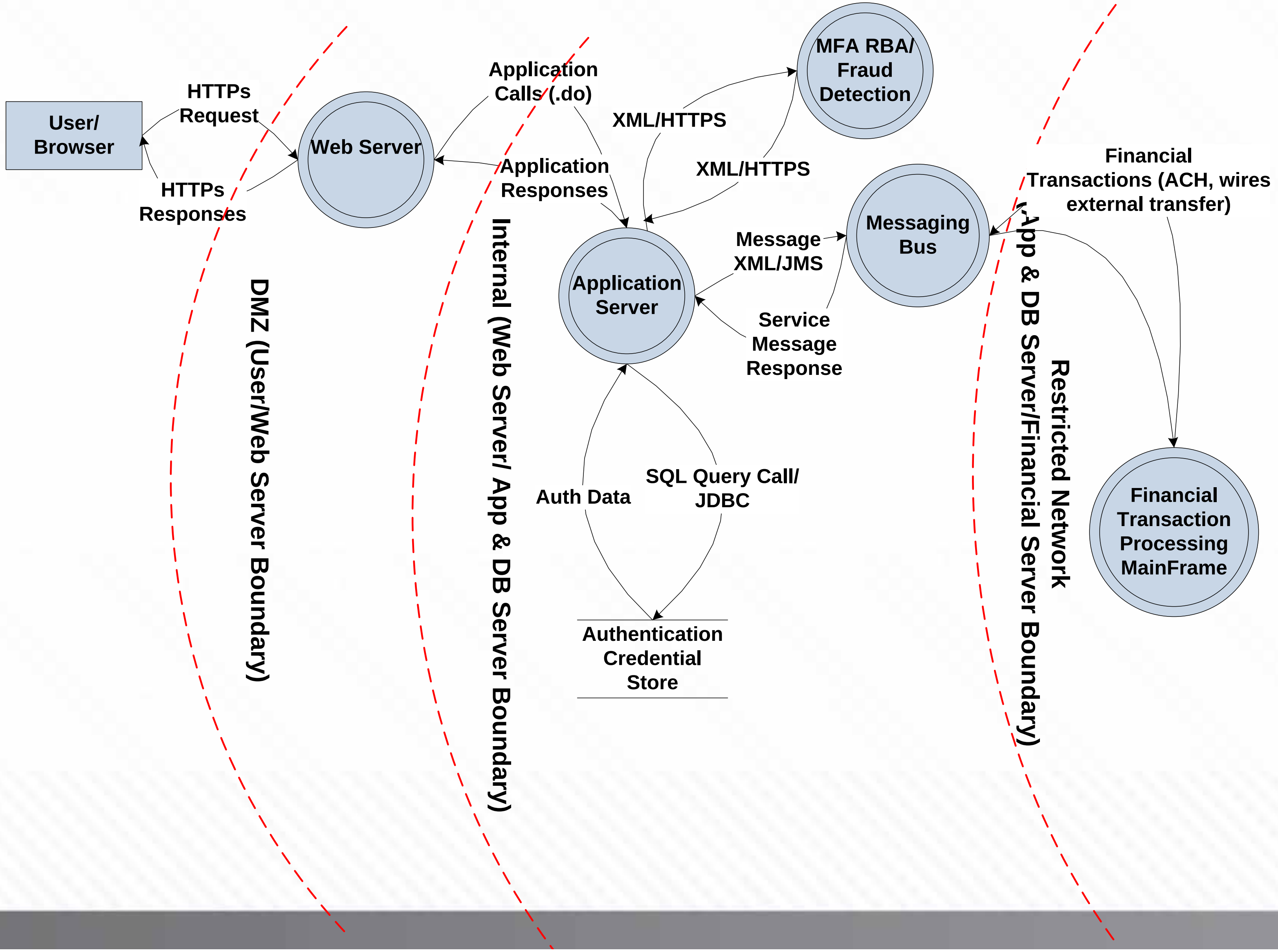
(3.3) Identify Assets, Data, Services, Hardware and Software

(3.4) Identify Data Entry Points and Trust Levels

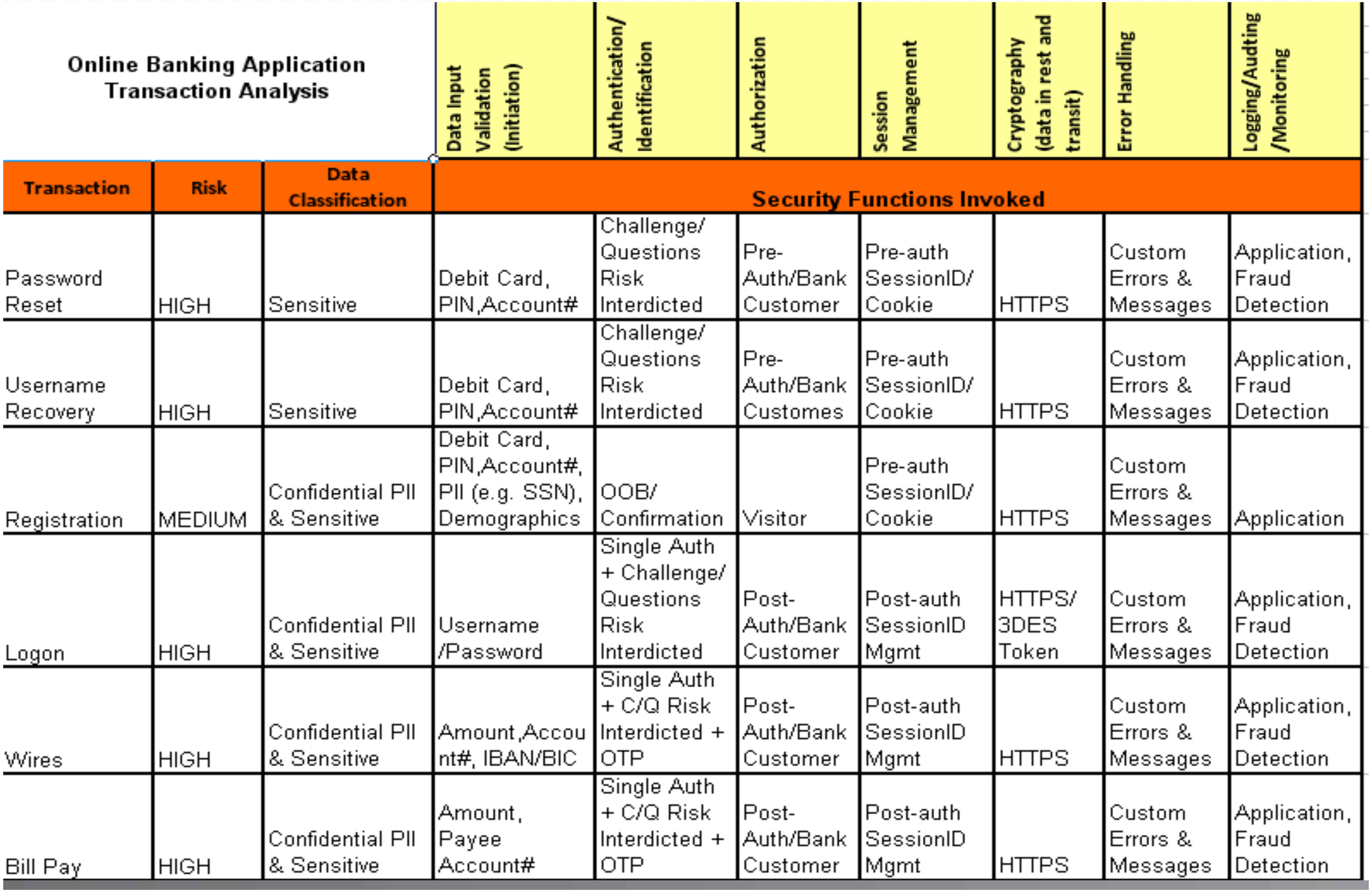
Output

Data Flow Diagrams
Access control matrix
List of assets including data and data sources
List of interfaces and trust levels
Mapping of use cases with actors and assets

Data Flow Diagramming (DFD)
On-line Banking Application Example

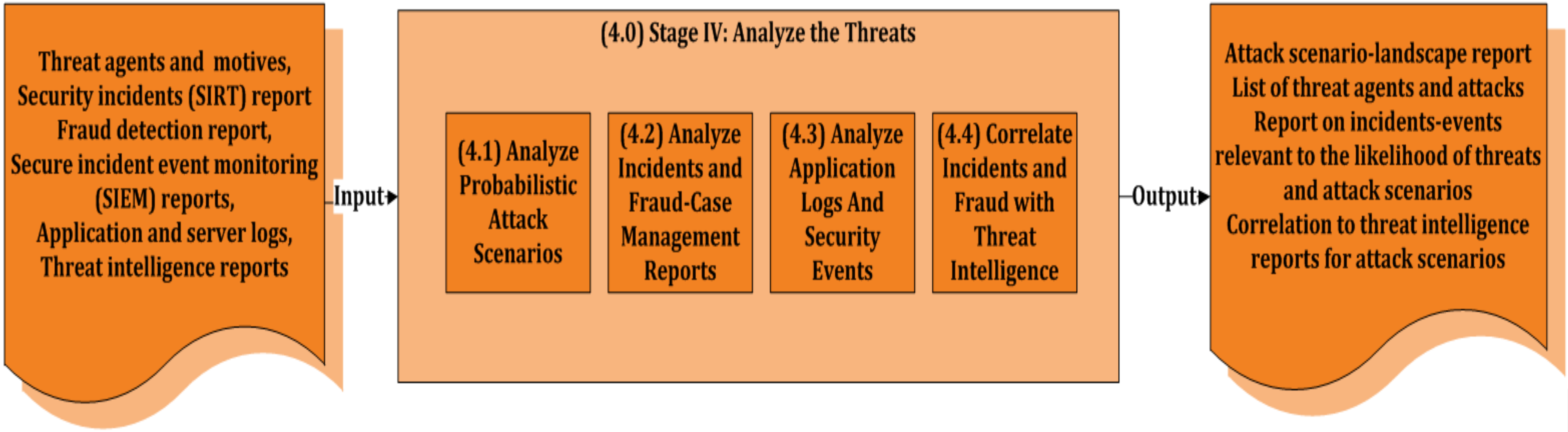


VerSprite Use Case to Countermeasure Tracking



Online Banking Application Transaction Analysis			Data Input Validation (Initiation)	Authentication/ Identification	Authorization	Session Management	Cryptography (data in rest and transit)	Error Handling	Logging/Audting /Monitoring
Transaction	Risk	Data Classification	Security Functions Invoked						
Password Reset	HIGH	Sensitive	Debit Card, PIN,Account#	Challenge/ Questions Risk Interdicted	Pre-Auth/Bank Customer	Pre-auth SessionID/ Cookie	HTTPS	Custom Errors & Messages	Application, Fraud Detection
Username Recovery	HIGH	Sensitive	Debit Card, PIN,Account#	Challenge/ Questions Risk Interdicted	Pre-Auth/Bank Customes	Pre-auth SessionID/ Cookie	HTTPS	Custom Errors & Messages	Application, Fraud Detection
Registration	MEDIUM	Confidential PII & Sensitive	Debit Card, PIN,Account#, PII (e.g. SSN), Demographics	OOB/ Confirmation	Visitor	Pre-auth SessionID/ Cookie	HTTPS	Custom Errors & Messages	Application
Logon	HIGH	Confidential PII & Sensitive	Username /Password	Single Auth + Challenge/ Questions Risk Interdicted	Post-Auth/Bank Customer	Post-auth SessionID Mgmt	HTTPS/ 3DES Token	Custom Errors & Messages	Application, Fraud Detection
Wires	HIGH	Confidential PII & Sensitive	Amount,Account#, IBAN/BIC	Single Auth + C/Q Risk Interdicted + OTP	Post-Auth/Bank Customer	Post-auth SessionID Mgmt	HTTPS	Custom Errors & Messages	Application, Fraud Detection
Bill Pay	HIGH	Confidential PII & Sensitive	Amount, Payee Account#	Single Auth + C/Q Risk Interdicted + OTP	Post-Auth/Bank Customer	Post-auth SessionID Mgmt	HTTPS	Custom Errors & Messages	Application, Fraud Detection

Stage 4 Threat Intelligence/ Analysis



Threat agents and motives,
Security incidents (SIRT) report
Fraud detection report,
Secure incident event monitoring (SIEM) reports,
Application and server logs,
Threat intelligence reports

Input

(4.0) Stage IV: Analyze the Threats

(4.1) Analyze Probabilistic Attack Scenarios

(4.2) Analyze Incidents and Fraud-Case Management Reports

(4.3) Analyze Application Logs And Security Events

(4.4) Correlate Incidents and Fraud with Threat Intelligence

Output

Attack scenario-landscape report
List of threat agents and attacks
Report on incidents-events relevant to the likelihood of threats and attack scenarios
Correlation to threat intelligence reports for attack scenarios

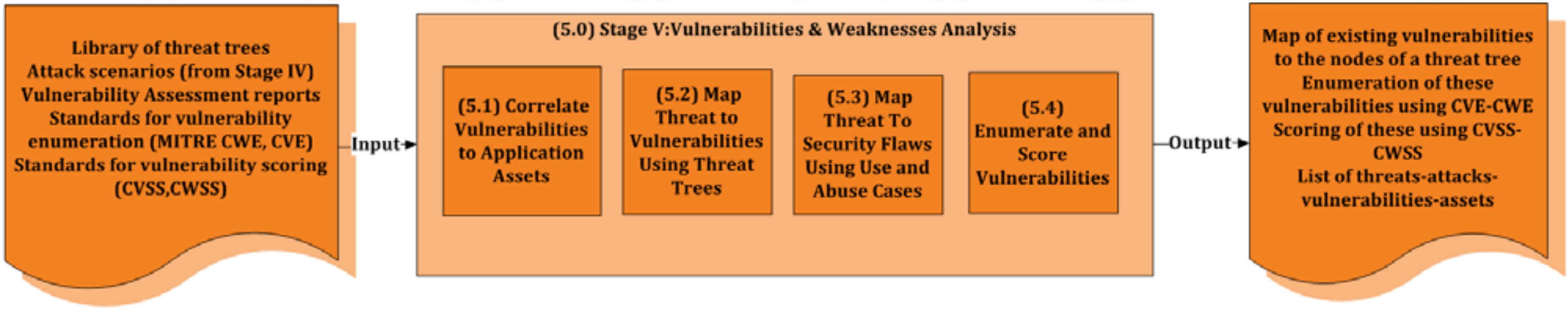
Threat Intelligence is Golden

- **Threat Enumeration Based upon Good Intel**
  - Threats based upon known intel
  - Prior assessment info (where applicable & useful)
  - Other application assessments from 3rd parties
  - SIEM feeds/ Syslog data/ Application Logs/ WAF logs
    - Denote attacks but will reveal overarching threats
  - Threat Intel/ Feeds
  - Security Operations/ Incident Reports
    - Personnel/ Infrastructure
- **Threat examples:**
  - IP Theft
  - Data Theft
  - Sabotage
  - Infrastructure compromise
  - Ransom

Threat Analysis Prefaces Attack Enumeration

- Threat analysis will lead to attack enumeration
  - PII theft
    - XSS
    - SQL Injection
    - MITM
  - Sabotage driven threats
    - CMS exploits to web application (Zope, Joomla, Mambo, etc)
    - FTP Brute Force attacks
    - iFrame Injection attacks
  - Malware upload
- Identify most likely attack vectors
  - Address entire application footprint (email, client app, etc)
  - Web Forms/ Fields
  - WSDLs/ SWF Objects
  - Compiled Libraries/ Named Pipes

Stage 5 Walkthru – Vuln Analysis



Library of threat trees
Attack scenarios (from Stage IV)
Vulnerability Assessment reports
Standards for vulnerability enumeration (MITRE CWE, CVE)
Standards for vulnerability scoring (CVSS,CWSS)

Input

(5.0) Stage V:Vulnerabilities & Weaknesses Analysis

(5.1) Correlate Vulnerabilities to Application Assets

(5.2) Map Threat to Vulnerabilities Using Threat Trees

(5.3) Map Threat To Security Flaws Using Use and Abuse Cases

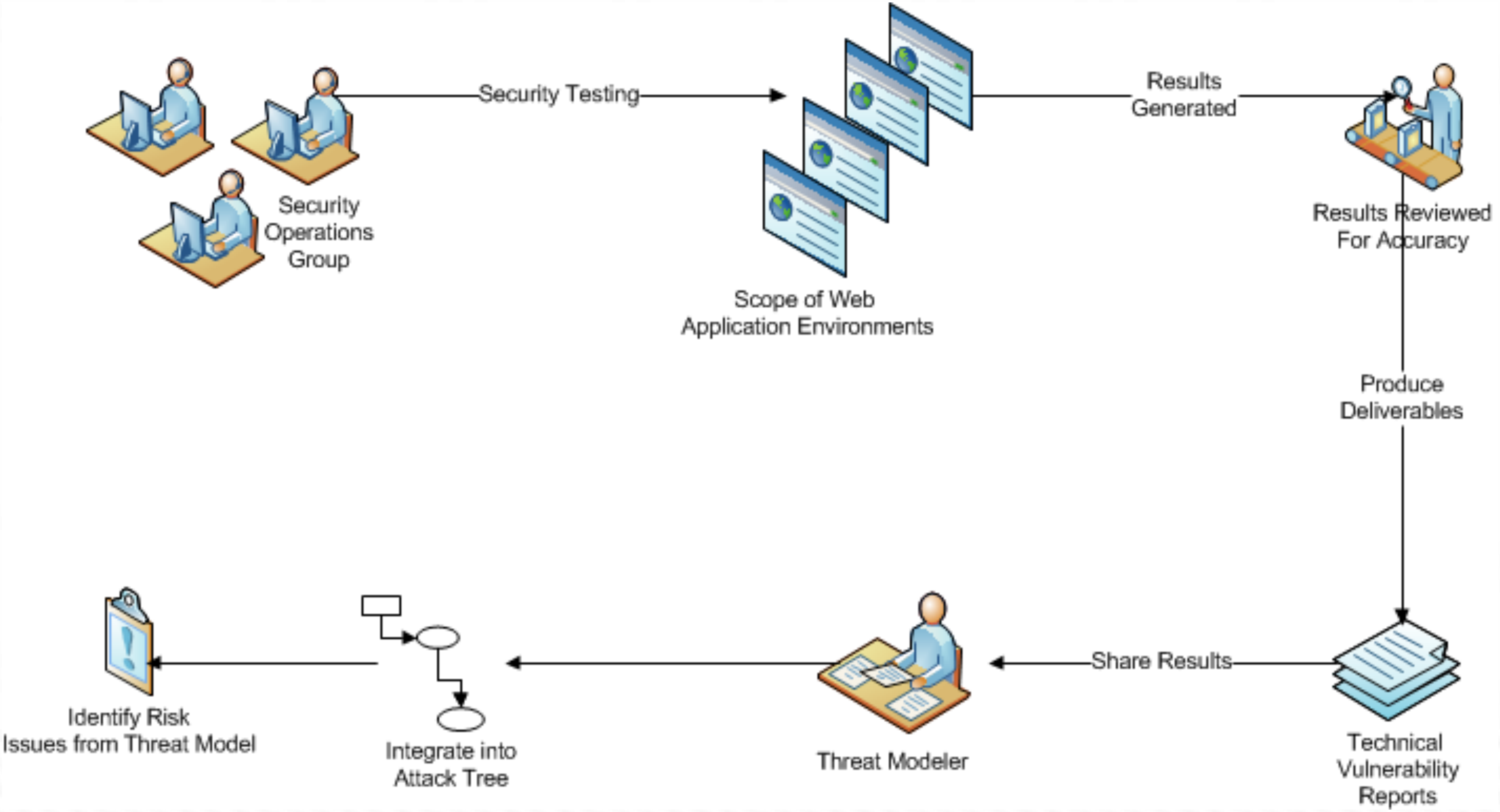
(5.4) Enumerate and Score Vulnerabilities

Output

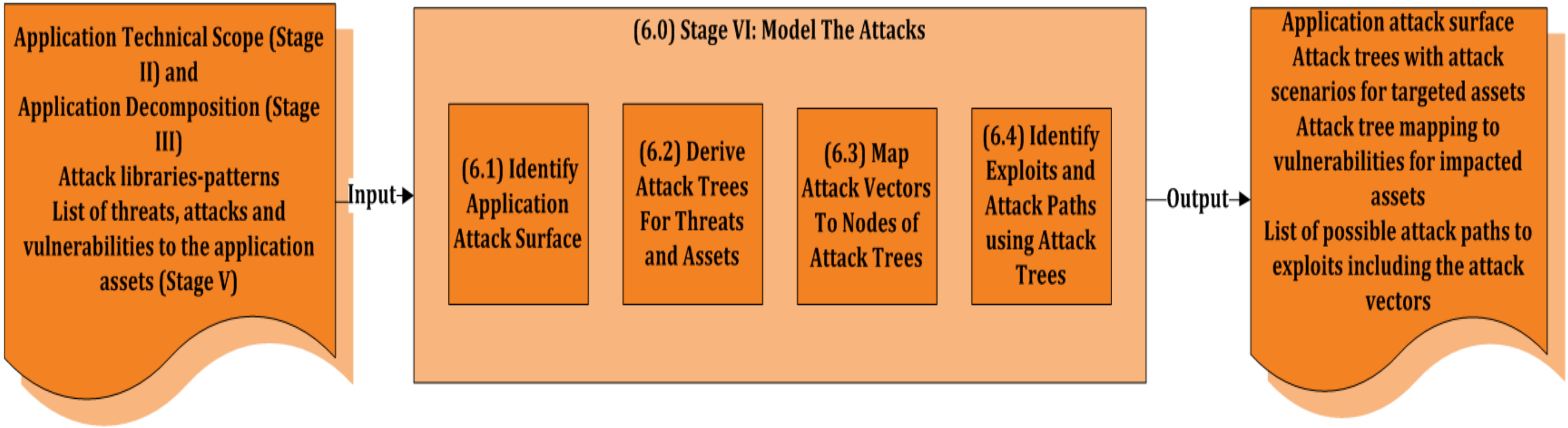
Map of existing vulnerabilities to the nodes of a threat tree
Enumeration of these vulnerabilities using CVE-CWE
Scoring of these using CVSS-CWSS
List of threats-attacks-vulnerabilities-assets

VerSprite

SecOps Convergence of Vulnerability Mgt.


Security Testing
Results Generated
Security Operations Group
Scope of Web Application Environments
Results Reviewed For Accuracy
Produce Deliverables
Share Results
Identify Risk Issues from Threat Model
Integrate into Attack Tree
Threat Modeler
Technical Vulnerability Reports

Stage 6 Walkthru – Attack Enumeration



Application Technical Scope (Stage II) and
Application Decomposition (Stage III)
Attack libraries-patterns
List of threats, attacks and vulnerabilities to the application assets (Stage V)

Input

(6.0) Stage VI: Model The Attacks

(6.1) Identify Application Attack Surface

(6.2) Derive Attack Trees For Threats and Assets

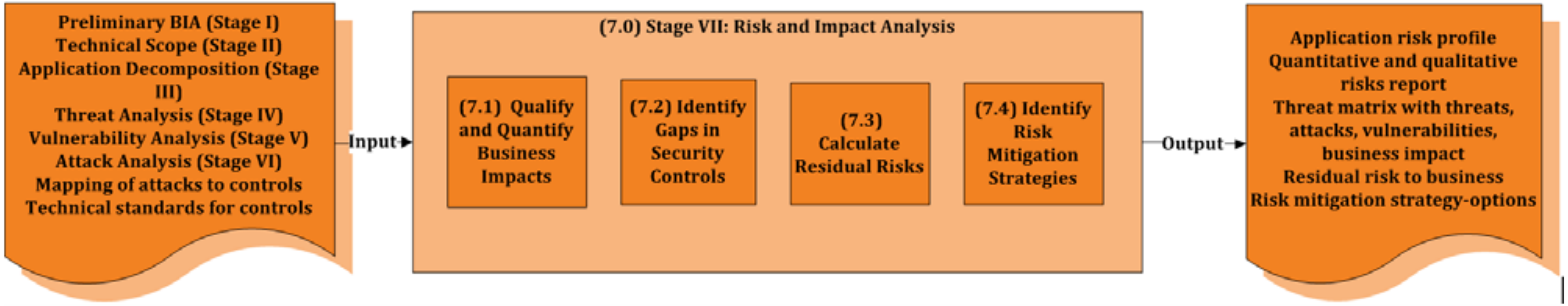
(6.3) Map Attack Vectors To Nodes of Attack Trees

(6.4) Identify Exploits and Attack Paths using Attack Trees

Output

Application attack surface
Attack trees with attack scenarios for targeted assets
Attack tree mapping to vulnerabilities for impacted assets
List of possible attack paths to exploits including the attack vectors

Stage 7– Residual Risk Analysis



Preliminary BIA (Stage I)
Technical Scope (Stage II)
Application Decomposition (Stage III)
Threat Analysis (Stage IV)
Vulnerability Analysis (Stage V)
Attack Analysis (Stage VI)
Mapping of attacks to controls
Technical standards for controls

Input

(7.0) Stage VII: Risk and Impact Analysis

(7.1) Qualify and Quantify Business Impacts

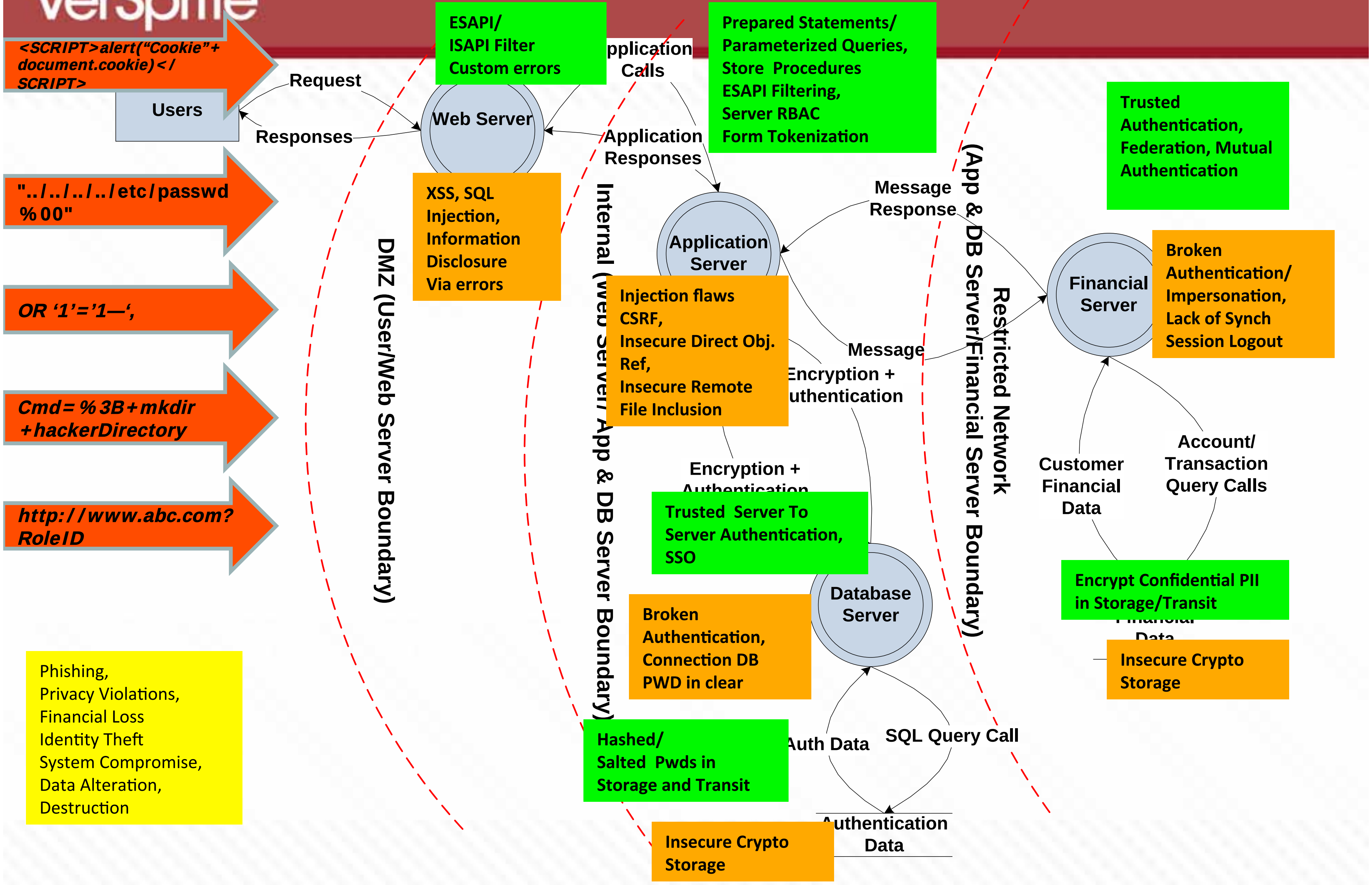
(7.2) Identify Gaps in Security Controls

(7.3) Calculate Residual Risks

(7.4) Identify Risk Mitigation Strategies

Output

Application risk profile
Quantitative and qualitative risks report
Threat matrix with threats, attacks, vulnerabilities, business impact
Residual risk to business
Risk mitigation strategy-options



<SCRIPT>alert("Cookie"+ document.cookie)</ SCRIPT>

"../../../../etc/passwd %00"

OR '1'='1—',

Cmd=%3B+mkdir +hackerDirectory

http://www.abc.com? RoleID

Users

Request

Responses

ESAPI/
ISAPI Filter
Custom errors

Web Server

XSS, SQL
Injection,
Information
Disclosure
Via errors

DMZ (User/Web Server Boundary)

pplication
Calls

Application
Responses

Internal (Web Server/ App & DB Server Boundary)

Prepared Statements/
Parameterized Queries,
Store Procedures
ESAPI Filtering,
Server RBAC
Form Tokenization

Application
Server

Injection flaws
CSRF,
Insecure Direct Obj. Ref,
Insecure Remote
File Inclusion

Encryption +
Authentication

Trusted Server To
Server Authentication,
SSO

Encryption +
uthentication

Database
Server

Broken
Authentication,
Connection DB
PWD in clear

Hashed/
Salted Pwds in
Storage and Transit

Auth Data

SQL Query Call

Authentication
Data

Insecure Crypto
Storage

Message
Response

Message

(App & DB Server/Financial Server Boundary)

Restricted Network

Trusted
Authentication,
Federation, Mutual
Authentication

Financial
Server

Broken
Authentication/
Impersonation,
Lack of Synch
Session Logout

Customer
Financial
Data

Account/
Transaction
Query Calls

Encrypt Confidential PII
in Storage/Transit

Financial
Data

Insecure Crypto
Storage

Phishing,
Privacy Violations,
Financial Loss
Identity Theft
System Compromise,
Data Alteration,
Destruction

The PASTA™ Risk Recipe

- Focus on **the application as** business-asset target
- Risk !=t * v * i
- Risk! = t * v * i * p

- Attack simulation enhances (*p*) probability coefficients
- Considers both inherent countermeasures & those to be developed
- Focused on minimizing risks to applications and associated impacts to business

- $R_{risk} =[(t_{p} * v_{p})/c] * i$

VerSprite
Navigate Beyond Risk

Q&A

QUESTIONS
ANSWERS

tonyuv@versprite.com
@t0nyuv
@versprite